

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<pre> Spanning tree enabled protocol rstp Root ID Priority 32768 Address 000d.eca3.9f01 Cost 4 Port 4105 (port-channel10) Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32770 (priority 32768 sys-id-ext 2) Address 0022.5579.7641 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Interface Role Sts Cost Prio.Nbr Type ----- Po10 Root FWD 2 128.4105 (vPC peer-link) P2p Po20 Desg FWD 1 128.4115 (vPC) P2p Po30 Root FWD 1 128.4125 (vPC) P2p </pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-59:L2-64</p>	<pre> Spanning tree enabled protocol rstp Root ID Priority 32768 Address 001c.7301.07b9 Cost 1999 (Ext) 0 (Int) Port 101 (Port-Channel12) Hello Time 2.000 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32768 (priority 32768 sys-id-ext 0) Address 001c.7304.195b Hello Time 2.000 sec Max Age 20 sec Forward Delay 15 sec Interface Role State Cost Prio.Nbr Type ----- Et4 designated forwarding 20000 128.4 P2p Et5 designated forwarding 20000 128.5 P2p Et6 designated forwarding 20000 128.6 P2p Et23 designated forwarding 20000 128.23 P2p Et26 designated forwarding 20000 128.26 P2p Et32 designated forwarding 2000 128.32 P2p </pre> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 983.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 861; Arista User Manual, v. 4.11.1 (1/11/13), at 679; Arista User Manual v. 4.10.3 (10/22/12), at 593; Arista User Manual v. 4.9.3.2 (5/3/12), at 512; Arista User Manual v. 4.8.2 (11/18/11), at 386; Arista User Manual v. 4.7.3 (7/18/11), at 275; Arista User Manual v. 4.6.0 (12/22/2010), at 268</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display detailed information about the STP configuration:</p> <pre>switch(config)# show spanning-tree detail</pre> <p>VLAN0001 is executing the rstp compatible Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 1, address 0022.5579.7641</p> <p>Configured hello time 2, max age 20, forward delay 15</p> <p>Current root has priority 32769, address 000d.eca3.9f01</p> <p>Root port is 4105 (port-channel10), cost of root path is 4</p> <p>Topology change flag not set, detected flag not set</p> <p>Number of topology changes 1 last change occurred 20:24:36 ago</p> <p>from port-channel10</p> <p>Times: hold 1, topology change 35, notification 2</p> <p>hello 2, max age 20, forward delay 15</p> <p>Timers: hello 0, topology change 0, notification 0</p> <p>Port 4105 (port-channel10, VPC Peer-link) of VLAN0001 is root forwarding</p> <p>Port path cost 2, Port priority 128, Port Identifier 128.4105</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4105, designated path cost 2</p> <p>Timers: message age 16, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 36729, received 36739</p> <p>Port 4115 (port-channel20, VPC) of VLAN0001 is designated forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4115</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4115, designated path cost 2</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Port 4125 (port-channel30, VPC) of VLAN0001 is root forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4125</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 000d.eca3.9f01</p> <p>Designated port id is 128.4125, designated path cost 0</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 74-75Release 6.x (2013), at 73</p>	<ul style="list-style-type: none"> This command displays STP data, including an information block for each interface running STP. <pre>switch>show spanning-tree vlan 1000 detail</pre> <p>MST0 is executing the rstp Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 0, address 001c.7304.195b</p> <p>Configured hello time 2.000, max age 20, forward delay 15, transmit hold-count 6</p> <p>Current root has priority 32768, address 001c.7301.07b9</p> <p>Root port is 101 (Port-Channel12), cost of root path is 1999 (Ext) 0 (Int)</p> <p>Number of topology changes 4109 last change occurred 1292651 seconds ago</p> <p>from Ethernet13</p> <p>Port 4 (Ethernet4) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.4.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.4, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, internal</p> <p>BPDU: sent 452252, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Port 5 (Ethernet5) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.5.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, Internal</p> <p>BPDU: sent 1006266, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 984.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 862; Arista User Manual, v. 4.11.1 (1/11/13), at 680; Arista User Manual v. 4.10.3 (10/22/12), at 594; Arista User Manual v. 4.9.3.2 (5/3/12), at 513; Arista User Manual v. 4.8.2 (11/18/11), at 387; Arista User Manual v. 4.7.3 (7/18/11), at 276.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display detailed information about the STP configuration:</p> <pre>switch(config)# show spanning-tree detail</pre> <p>VLAN0001 is executing the rstp compatible Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 1, address 0022.5579.7641</p> <p>Configured hello time 2, max age 20, forward delay 15</p> <p>Current root has priority 32769, address 000d.eca3.9f01</p> <p>Root port is 4105 (port-channel10), cost of root path is 4</p> <p>Topology change flag not set, detected flag not set</p> <p>Number of topology changes 1 last change occurred 20:24:36 ago</p> <p>from port-channel10</p> <p>Times: hold 1, topology change 35, notification 2</p> <p>hello 2, max age 20, forward delay 15</p> <p>Timers: hello 0, topology change 0, notification 0</p> <p>Port 4105 (port-channel10, VPC Peer-link) of VLAN0001 is root forwarding</p> <p>Port path cost 2, Port priority 128, Port Identifier 128.4105</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4105, designated path cost 2</p> <p>Timers: message age 16, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 36729, received 36739</p> <p>Port 4115 (port-channel20, VPC) of VLAN0001 is designated forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4115</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 0022.5579.7341</p> <p>Designated port id is 128.4115, designated path cost 2</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Port 4125 (port-channel30, VPC) of VLAN0001 is root forwarding</p> <p>Port path cost 1, Port priority 128, Port Identifier 128.4125</p> <p>Designated root has priority 32769, address 000d.eca3.9f01</p> <p>Designated bridge has priority 32769, address 000d.eca3.9f01</p> <p>Designated port id is 128.4125, designated path cost 0</p> <p>Timers: message age 0, forward delay 0, hold 0</p> <p>Number of transitions to forwarding state: 0</p> <p>Link type is point-to-point by default</p> <p>BPDU: sent 0, received 0</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-71:L2-72</p>	<ul style="list-style-type: none"> This command displays STP data, including an information block for each interface running STP. <pre>switch>show spanning-tree vlan 1000 detail</pre> <p>MST0 is executing the rstp Spanning Tree protocol</p> <p>Bridge Identifier has priority 32768, sysid 0, address 001c.7304.195b</p> <p>Configured hello time 2.000, max age 20, forward delay 15, transmit hold-count 6</p> <p>Current root has priority 32768, address 001c.7301.07b9</p> <p>Root port is 101 (Port-Channel12), cost of root path is 1999 (Ext) 0 (Int)</p> <p>Number of topology changes 4109 last change occurred 1292651 seconds ago</p> <p>from Ethernet13</p> <p>Port 4 (Ethernet4) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.4.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.4, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, internal</p> <p>BPDU: sent 452252, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Port 5 (Ethernet5) of MST0 is designated forwarding</p> <p>Port path cost 20000, Port priority 128, Port Identifier 128.5.</p> <p>Designated root has priority 32768, address 001c.7301.07b9</p> <p>Designated bridge has priority 32768, address 001c.7304.195b</p> <p>Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int)</p> <p>Timers: message age 1, forward delay 15, hold 20</p> <p>Number of transitions to forwarding state: 1</p> <p>Link type is point-to-point by default, Internal</p> <p>BPDU: sent 1006266, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0</p> <p>Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <p>Arista User Manual v. 4.14.3F (Rev. 2) (10/2/2014), at 984.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 862; Arista User Manual, v. 4.11.1 (1/11/13), at 680; Arista User Manual v. 4.10.3 (10/22/12), at 594; Arista User Manual v. 4.9.3.2 (5/3/12), at 513; Arista User Manual v. 4.8.2 (11/18/11), at 387; Arista User Manual v. 4.7.3 (7/18/11), at 276.</p>

Copyright Registration Information	Cisco	Arista																																												
	<p>This example shows how to display STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/2</pre> <table><thead><tr><th>Vlan</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>VLAN0001</td><td>Altn</td><td>BLK</td><td>20000</td><td>128.1025</td><td>P2p</td></tr><tr><td>VLAN0002</td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1025</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display STP information about a specified interface when you are running MST:</p> <pre>switch(config)# show spanning-tree interface ethernet 2/50</pre> <table><thead><tr><th>Mst</th><th>Instance</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0000</td><td></td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1281</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display detailed STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/1 detail</pre> <p>Port 1025 (Ethernet8/1) of VLAN0001 is alternate blocking Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 28672, address 0018.bad8.239d Designated bridge has priority 28672, address 0018.bad8.239d Designated port id is 128.1281, designated path cost 0 Timers: message age 15, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDU: sent 4657, received 188</p> <p>Port 1025 (Ethernet8/1) of VLAN0002 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 32770, address 0018.bad7.fc15 Designated bridge has priority 32770, address 0018.bad7.fc15 Designated port id is 128.1025, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDU: sent 4838, received 0</p>	Vlan	Role	Sts	Cost	Prio.Nbr	Type	VLAN0001	Altn	BLK	20000	128.1025	P2p	VLAN0002	Desg	FWD	20000	128.1025	P2p	Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type	MST0000		Desg	FWD	20000	128.1281	P2p	<p>Examples</p> <ul style="list-style-type: none">This command displays an STP table for Ethernet 5 interface. <pre>switch#show spanning-tree interface ethernet 5</pre> <table><thead><tr><th>Instance</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0</td><td>designated</td><td>forwarding</td><td>20000</td><td>128.5</td><td>P2p</td></tr></tbody></table> <pre>switch></pre> <ul style="list-style-type: none">This command displays a data block for Ethernet interface 5. <pre>switch#show spanning-tree interface ethernet 5 detail</pre> <p>Port 5 (Ethernet5) of MST0 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.5. Designated root has priority 32768, address 001c.7301.07b9 Designated bridge has priority 32768, address 001c.7304.195b Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int) Timers: message age 1, forward delay 15, hold 20 Number of transitions to forwarding state: 1 Link type is point-to-point by default, Internal BPDU: sent 1008766, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0 Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400<pre>switch></pre></p>	Instance	Role	State	Cost	Prio.Nbr	Type	MST0	designated	forwarding	20000	128.5	P2p
Vlan	Role	Sts	Cost	Prio.Nbr	Type																																									
VLAN0001	Altn	BLK	20000	128.1025	P2p																																									
VLAN0002	Desg	FWD	20000	128.1025	P2p																																									
Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type																																								
MST0000		Desg	FWD	20000	128.1281	P2p																																								
Instance	Role	State	Cost	Prio.Nbr	Type																																									
MST0	designated	forwarding	20000	128.5	P2p																																									
Cisco NX-OS 6.2		Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 988.																																												
Effective date of registration: 11/13/2014	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 77.	See also Arista User Manual v. 4.12.3 (7/17/13), at 866; Arista User Manual, v. 4.11.1 (1/11/13), at 684; Arista User Manual v. 4.10.3 (10/22/12), at 598; Arista User Manual v. 4.9.3.2 (5/3/12), at 517; Arista User Manual v. 4.8.2 (11/18/11), at 391; Arista User Manual v. 4.7.3 (7/18/11), at 280.																																												

Copyright Registration Information	Cisco	Arista																																												
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>This example shows how to display STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/2</pre> <table><thead><tr><th>Vlan</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>VLAN0001</td><td>Altn</td><td>BLK</td><td>20000</td><td>128.1025</td><td>P2p</td></tr><tr><td>VLAN0002</td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1025</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display STP information about a specified interface when you are running MST:</p> <pre>switch(config)# show spanning-tree interface ethernet 2/50</pre> <table><thead><tr><th>Mst</th><th>Instance</th><th>Role</th><th>Sts</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0000</td><td></td><td>Desg</td><td>FWD</td><td>20000</td><td>128.1281</td><td>P2p</td></tr></tbody></table> <p>This example shows how to display detailed STP information about a specified interface when you are running Rapid PVST+:</p> <pre>switch(config)# show spanning-tree interface ethernet 8/1 detail</pre> <p>Port 1025 (Ethernet8/1) of VLAN0001 is alternate blocking Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 28672, address 0018.bad8.239d Designated bridge has priority 28672, address 0018.bad8.239d Designated port id is 128.1281, designated path cost 0 Timers: message age 15, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDU: sent 4657, received 188</p> <p>Port 1025 (Ethernet8/1) of VLAN0002 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.1025 Designated root has priority 32770, address 0018.bad7.fc15 Designated bridge has priority 32770, address 0018.bad7.fc15 Designated port id is 128.1025, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default The port type is network by default. BPDU: sent 4838, received 0</p>	Vlan	Role	Sts	Cost	Prio.Nbr	Type	VLAN0001	Altn	BLK	20000	128.1025	P2p	VLAN0002	Desg	FWD	20000	128.1025	P2p	Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type	MST0000		Desg	FWD	20000	128.1281	P2p	<p>Examples</p> <ul style="list-style-type: none">This command displays an STP table for Ethernet 5 interface. <pre>switch#show spanning-tree interface ethernet 5</pre> <table><thead><tr><th>Instance</th><th>Role</th><th>State</th><th>Cost</th><th>Prio.Nbr</th><th>Type</th></tr></thead><tbody><tr><td>MST0</td><td>designated</td><td>forwarding</td><td>20000</td><td>128.5</td><td>P2p</td></tr></tbody></table> <pre>switch></pre> <ul style="list-style-type: none">This command displays a data block for Ethernet interface 5. <pre>switch#show spanning-tree interface ethernet 5 detail</pre> <p>Port 5 (Ethernet5) of MST0 is designated forwarding Port path cost 20000, Port priority 128, Port Identifier 128.5. Designated root has priority 32768, address 001c.7301.07b9 Designated bridge has priority 32768, address 001c.7304.195b Designated port id is 128.5, designated path cost 1999 (Ext) 0 (Int) Timers: message age 1, forward delay 15, hold 20 Number of transitions to forwarding state: 1 Link type is point-to-point by default, Internal BPDU: sent 1008766, received 0, taggedErr 0, otherErr 0, rateLimiterCount 0 Rate-Limiter: enabled, Window: 10 sec, Max-BPDU: 400</p> <pre>switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 988.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 866; Arista User Manual, v. 4.11.1 (1/11/13), at 684; Arista User Manual v. 4.10.3 (10/22/12), at 598; Arista User Manual v. 4.9.3.2 (5/3/12), at 517; Arista User Manual v. 4.8.2 (11/18/11), at 391; Arista User Manual v. 4.7.3 (7/18/11), at 280.</p>	Instance	Role	State	Cost	Prio.Nbr	Type	MST0	designated	forwarding	20000	128.5	P2p
	Vlan	Role	Sts	Cost	Prio.Nbr	Type																																								
	VLAN0001	Altn	BLK	20000	128.1025	P2p																																								
VLAN0002	Desg	FWD	20000	128.1025	P2p																																									
Mst	Instance	Role	Sts	Cost	Prio.Nbr	Type																																								
MST0000		Desg	FWD	20000	128.1281	P2p																																								
Instance	Role	State	Cost	Prio.Nbr	Type																																									
MST0	designated	forwarding	20000	128.5	P2p																																									
	Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-74																																													

Copyright
Registration
Information

Cisco

Arista

```
switch# show spanning-tree mst

##### MST0    vlans mapped: 1-4094
Bridge          address 0018.bad7.fc15 priority    32768 (32768 sysid 0)
Root            this switch for the CIST
Regional Root   this switch
Operational      hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured       hello time 2 , forward delay 15, max age 20, max hops    20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Eth8/1         Desg FWD 20000    128.1025 P2p
Eth8/2         Desg FWD 20000    128.1026 P2p

This example shows how to display STP information about a specific MST instance:

switch# show spanning-tree mst 0

##### MST0    vlans mapped: 1-4094
Bridge          address 0018.bad7.fc15 priority    32768 (32768 sysid 0)
Root            this switch for the CIST
Regional Root   this switch
Operational      hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured       hello time 2 , forward delay 15, max age 20, max hops    20

Interface      Role Sts Cost      Prio.Nbr Type
-----
Eth8/1         Desg FWD 20000    128.1025 P2p
Eth8/2         Desg FWD 20000    128.1026 P2p

This example shows how to display detailed STP information about the MST protocol:

switch# show spanning-tree mst detail

##### MST0    vlans mapped: 1-4094
Bridge          address 0018.bad7.fc15 priority    32768 (32768 sysid 0)
Root            this switch for the CIST
Regional Root   this switch
Operational      hello time 2 , forward delay 15, max age 20, txholdcount 6
Configured       hello time 2 , forward delay 15, max age 20, max hops    20

Eth8/1 of MST0 is designated forwarding
Port info        port id 128.1025 priority 128 cost 20000
Designated root  address 0018.bad7.fc15 priority 32768 cost 0
Design. regional root address 0018.bad7.fc15 priority 32768 cost 0
Designated bridge address 0018.bad7.fc15 priority 32768 port id 128.1025
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 1379, received 3

Eth8/2 of MST0 is designated forwarding
Port info        port id 128.1026 priority 128 cost 20000
Designated root  address 0018.bad7.fc15 priority 32768 cost 0
Design. regional root address 0018.bad7.fc15 priority 32768 cost 0
Designated bridge address 0018.bad7.fc15 priority 32768 port id 128.1026
Timers: message expires in 0 sec, forward delay 0, forward transitions 1
Bpdus sent 1380, received 2
```

Cisco NX-OS 6.2

Effective date of
registration:
11/13/2014Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference
(2013), at 80.

Examples

- This command displays interface data blocks for MST instance 3.

```
switch# show spanning-tree mst 3 detail

##### MST3    vlans mapped: 3
Bridge          address 0011.2233.4402 priority    32771 (32768 sysid 3)
Root            address 0011.2233.4401 priority    32771 (32768 sysid 3)

Ethernet1 of MST3 is root forwarding
Port info        port id 128.1 priority 128 cost 2000
Designated root  address 0011.2233.4401 priority 32768 cost 0
Designated bridge address 0011.2233.4401 priority 32768 port id 128.1

Ethernet2 of MST3 is alternate discarding
Port info        port id 128.2 priority 128 cost 2000
Designated root  address 0011.2233.4401 priority 32768 cost 0
Designated bridge address 0011.2233.4401 priority 32768 port id 128.2

Ethernet3 of MST3 is designated forwarding
Port info        port id 128.3 priority 128 cost 2000
Designated root  address 0011.2233.4401 priority 32768 cost 0
Designated bridge address 0011.2233.4402 priority 32768 port id 128.3
```

- This command displays interface tables for all MST instances.

```
switch# show spanning-tree mst

##### MST0    vlans mapped: 1,4-4094
Bridge          address 0011.2233.4402 priority    32768 (32768 sysid 0)
Root            address 0011.2233.4401 priority    32768 (32768 sysid 0)
Regional Root   address 0011.2233.4401 priority    32768 (32768 sysid 0)

Interface      Role      State      Cost      Prio.Nbr Type
-----
Et1             root      forwarding 2000       128.1    P2p
Et2             alternate discarding 2000       128.2    P2p
Et3             designated forwarding 2000       128.3    P2p
Et4             designated forwarding 2000       128.4    P2p

##### MST2 vlans mapped: 2
Bridge          address 0011.2233.4402 priority    8194 (8192 sysid 2)
Root            this switch for MST2

Interface      Role      State      Cost      Prio.Nbr Type
-----
Et1             designated forwarding 2000       128.1    P2p
Et2             designated forwarding 2000       128.2    P2p
Et3             designated forwarding 2000       128.3    P2p
Et4             designated forwarding 2000       128.4    P2p

##### MST3 vlans mapped: 3
Bridge          address 0011.2233.4402 priority    32771 (32768 sysid 3)
Root            address 0011.2233.4401 priority    32771 (32768 sysid 3)

Interface      Role      State      Cost      Prio.Nbr Type
-----
Et1             root      forwarding 2000       128.1    P2p
Et2             alternate discarding 2000       128.2    P2p
Et3             designated forwarding 2000       128.3    P2p
Et4             designated forwarding 2000       128.4    P2p
```

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 990.

See also Arista User Manual v. 4.12.3 (7/17/13), at 867-68; Arista User Manual, v. 4.11.1 (1/11/13), at 685-86; Arista User Manual v. 4.10.3 (10/22/12), at 599-600; Arista User Manual v. 4.9.3.2 (5/3/12), at 518-19; Arista User Manual v. 4.8.2 (11/18/11), at 392-393; Arista User Manual

Copyright Registration Information	Cisco	Arista
		v. 4.7.3 (7/18/11), at; Arista User Manual v. 4.7.3 (7/18/11), at 281-82.

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>switch# show spanning-tree mst</p> <pre> ##### MST0 vlans mapped: 1-4094 Bridge address 0018.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20 Interface Role Sts Cost Prio.Nbr Type ----- Eths/1 Desg FWD 20000 128.1025 P2p Eths/2 Desg FWD 20000 128.1026 P2p </pre> <p>This example shows how to display STP information about a specific MST instance:</p> <pre> switch# show spanning-tree mst 0 ##### MST0 vlans mapped: 1-4094 Bridge address 0018.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20 Interface Role Sts Cost Prio.Nbr Type ----- Eths/1 Desg FWD 20000 128.1025 P2p Eths/2 Desg FWD 20000 128.1026 P2p </pre> <p>This example shows how to display detailed STP information about the MST protocol:</p> <pre> switch# show spanning-tree mst detail ##### MST0 vlans mapped: 1-4094 Bridge address 0018.bad7.fc15 priority 32768 (32768 sysid 0) Root this switch for the CIST Regional Root this switch Operational hello time 2 , forward delay 15, max age 20, txholdcount 6 Configured hello time 2 , forward delay 15, max age 20, max hops 20 Eths/1 of MST0 is designated forwarding Port info port id 128.1025 priority 128 cost 20000 Designated root address 0018.bad7.fc15 priority 32768 cost 0 Design. regional root address 0018.bad7.fc15 priority 32768 cost 0 Designated bridge address 0018.bad7.fc15 priority 32768 port id 128.1025 Timers: message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus sent 1379, received 3 Eths/2 of MST0 is designated forwarding Port info port id 128.1026 priority 128 cost 20000 Designated root address 0018.bad7.fc15 priority 32768 cost 0 Design. regional root address 0018.bad7.fc15 priority 32768 cost 0 Designated bridge address 0018.bad7.fc15 priority 32768 port id 128.1026 Timers: message expires in 0 sec, forward delay 0, forward transitions 1 Bpdus sent 1380, received 2 </pre>	<p>Examples</p> <ul style="list-style-type: none"> This command displays interface data blocks for MST instance 3. <pre> switch# show spanning-tree mst 3 detail ##### MST3 vlans mapped: 3 Bridge address 0011.2233.4402 priority 32771 (32768 sysid 3) Root address 0011.2233.4401 priority 32771 (32768 sysid 3) Ethernet1 of MST3 is root forwarding Port info port id 128.1 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 0 Designated bridge address 0011.2233.4401 priority 32768 port id 128.1 Ethernet2 of MST3 is alternate discarding Port info port id 128.2 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 0 Designated bridge address 0011.2233.4401 priority 32768 port id 128.2 Ethernet3 of MST3 is designated forwarding Port info port id 128.3 priority 128 cost 2000 Designated root address 0011.2233.4401 priority 32768 cost 2000 Designated bridge address 0011.2233.4402 priority 32768 port id 128.3 </pre> <ul style="list-style-type: none"> This command displays interface tables for all MST instances. <pre> switch# show spanning-tree mst ##### MST0 vlans mapped: 1,4-4094 Bridge address 0011.2233.4402 priority 32768 (32768 sysid 0) Root address 0011.2233.4401 priority 32768 (32768 sysid 0) Regional Root address 0011.2233.4401 priority 32768 (32768 sysid 0) Interface Role State Cost Prio.Nbr Type ----- Et1 root forwarding 2000 128.1 P2p Et2 alternate discarding 2000 128.2 P2p Et3 designated forwarding 2000 128.3 P2p Et4 designated forwarding 2000 128.4 P2p ##### MST2 vlans mapped: 2 Bridge address 0011.2233.4402 priority 8194 (8192 sysid 2) Root this switch for MST2 Interface Role State Cost Prio.Nbr Type ----- Et1 designated forwarding 2000 128.1 P2p Et2 designated forwarding 2000 128.2 P2p Et3 designated forwarding 2000 128.3 P2p Et4 designated forwarding 2000 128.4 P2p ##### MST3 vlans mapped: 3 Bridge address 0011.2233.4402 priority 32771 (32768 sysid 3) Root address 0011.2233.4401 priority 32771 (32768 sysid 3) Interface Role State Cost Prio.Nbr Type ----- Et1 root forwarding 2000 128.1 P2p Et2 alternate discarding 2000 128.2 P2p Et3 designated forwarding 2000 128.3 P2p Et4 designated forwarding 2000 128.4 P2p </pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 990.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 867-68; Arista User Manual, v. 4.11.1 (1/11/13), at 685-86; Arista User Manual v. 4.10.3 (10/22/12), at 599-600; Arista User Manual v. 4.9.3.2 (5/3/12), at 518-19; Arista User Manual v. 4.8.2 (11/18/11), at 392-393; Arista User Manual v. 4.7.3 (7/18/11), at; Arista User Manual v. 4.7.3 (7/18/11), at 281-82.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display information about the MST configuration:</p> <pre>switch)# show spanning-tree mst configuration</pre> <pre>Name: [mst-bldg-sj6/3] Revision: 1 Instances Configured: 3 Instance Vlans mapped ----- 0 1 2000 2-2000 4094 2001-4094 -----</pre> <p>This example shows how to display the MD5 digest included in the current MST configuration:</p> <pre>switch)# show spanning-tree mst configuration digest</pre> <pre>Name [mst-config] Revision 10 Instances configured 25 Digest 0x40D5ECA178C657835C83BB4B16723192 Pre-std Digest 0x27BF112A75B72781ED928D9EC5BB4251</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 81.</p>	<p>Examples</p> <ul style="list-style-type: none"> This command displays the MST region's VLAN-to-instance map. <pre>switch>show spanning-tree mst configuration</pre> <pre>Name [] Revision 0 Instances configured 3 Instance Vlans mapped ----- 0 1,4-4094 2 2 3 3 ----- switch></pre> <ul style="list-style-type: none"> This command displays the MST region's configuration digest. <pre>switch>show spanning-tree mst configuration digest</pre> <pre>Name [] Revision 0 Instances configured 1 Digest 0xAC36177F50283CD4B83821D8AB26DE62 switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>This example shows how to display information about the MST configuration:</p> <pre>switch)# show spanning-tree mst configuration</pre> <pre>Name: [mst-bldg-sj6/3] Revision: 1 Instances Configured: 3 Instance Vlans mapped ----- 0 1 2000 2-2000 4094 2001-4094 -----</pre> <p>This example shows how to display the MD5 digest included in the current MST configuration:</p> <pre>switch)# show spanning-tree mst configuration digest</pre> <pre>Name [mst-config] Revision 10 Instances configured 25 Digest 0x40D5ECA178C657835C83BBCE16723192 Pre-std Digest 0x27BF112A75B72781ED928D9EC5BB4251</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-78</p>	<p>Examples</p> <ul style="list-style-type: none"> This command displays the MST region's VLAN-to-instance map. <pre>switch>show spanning-tree mst configuration</pre> <pre>Name [] Revision 0 Instances configured 3 Instance Vlans mapped ----- 0 1,4-4094 2 2 3 3 ----- switch></pre> <ul style="list-style-type: none"> This command displays the MST region's configuration digest. <pre>switch>show spanning-tree mst configuration digest</pre> <pre>Name [] Revision 0 Instances configured 1 Digest 0xAC36177F50283CD4B83821D8AB26DE62 switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 991.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 869; Arista User Manual, v. 4.11.1 (1/11/13), at 687; Arista User Manual v. 4.10.3 (10/22/12), at 601; Arista User Manual v. 4.9.3.2 (5/3/12), at 520; Arista User Manual v. 4.8.2 (11/18/11), at 394; Arista User Manual v. 4.7.3 (7/18/11), at 283.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Examples</p> <p>This example shows how to display information for the root bridge:</p> <pre>switch(config)# show spanning-tree root</pre> <pre>MST Instance Root ID Cost Time Age Dly Root Port ----- MST0000 32768 0018.bad7.fc15 0 2 20 15 This bridge is root</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 82-83.</p>	<p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 994.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 872; Arista User Manual, v. 4.11.1 (1/11/13), at 690; Arista User Manual v. 4.10.3 (10/22/12), at 604; Arista User Manual v. 4.9.3.2 (5/3/12), at 523; Arista User Manual v. 4.8.2 (11/18/11), at 397; Arista User Manual v. 4.7.3 (7/18/11), at 286.</p>

Copyright Registration Information	Cisco	Arista														
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Examples This example shows how to display information for the root bridge:</p> <pre>switch(config)# show spanning-tree root</pre> <table><thead><tr><th>MST Instance</th><th>Root ID</th><th>Cost</th><th>Time</th><th>Age</th><th>Dly</th><th>Root Port</th></tr></thead><tbody><tr><td>MST0000</td><td>32768 0018.bad7.fc15</td><td>0</td><td>2</td><td>20</td><td>15</td><td>This bridge is root</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-79:L2-80</p>	MST Instance	Root ID	Cost	Time	Age	Dly	Root Port	MST0000	32768 0018.bad7.fc15	0	2	20	15	This bridge is root	<p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 994.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 872; Arista User Manual, v. 4.11.1 (1/11/13), at 690; Arista User Manual v. 4.10.3 (10/22/12), at 604; Arista User Manual v. 4.9.3.2 (5/3/12), at 523; Arista User Manual v. 4.8.2 (11/18/11), at 397; Arista User Manual v. 4.7.3 (7/18/11), at 286.</p>
MST Instance	Root ID	Cost	Time	Age	Dly	Root Port										
MST0000	32768 0018.bad7.fc15	0	2	20	15	This bridge is root										
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>This example shows how to display information about the number of VLANs configured on the device:</p> <pre>switch# show vlan summary</pre> <pre>Number of existing VLANs : 9 Number of existing user VLANs : 9 Number of existing extended VLANs : 0</pre> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 94.</p>	<p>Example</p> <ul style="list-style-type: none">This command displays the number of VLANs on the switch. <pre>switch>show vlan summary</pre> <pre>Number of existing VLANs : 18</pre> <pre>switch></pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 791.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 638; Arista User Manual, v. 4.11.1 (1/11/13), at 492; Arista User Manual v. 4.10.3 (10/22/12), at 410; Arista User Manual v. 4.9.3.2 (5/3/12), at 345.</p>														

Copyright Registration Information	Cisco	Arista																																
<div>Cisco NX-OS 5.0</div> <div>Effective date of registration: 11/13/2014</div>	<div>This example shows how to display information about the number of VLANs configured on the device:</div> <div><pre>switch# show vlan summary Number of existing VLANs : 9 Number of existing user VLANs : 9 Number of existing extended VLANs : 0</pre></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-90</div>	<div>Example</div> <div><ul style="list-style-type: none">This command displays the number of VLANs on the switch.</div> <div><pre>switch>show vlan summary Number of existing VLANs : 18 switch></pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 791.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 638; Arista User Manual, v. 4.11.1 (1/11/13), at 492; Arista User Manual v. 4.10.3 (10/22/12), at 410; Arista User Manual v. 4.9.3.2 (5/3/12), at 345.</div>																																
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div>Examples</div> <div>This example shows how to display information about all private VLANs on the device:</div> <div><pre>switch(config)# show vlan private-vlan</pre><table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>200</td><td>201</td><td>isolated</td><td>Eth2/26, Eth2/27</td></tr><tr><td>200</td><td>202</td><td>community</td><td>Eth2/26, Eth2/28</td></tr></tbody></table></div> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 94.</div>	Primary	Secondary	Type	Ports	200	201	isolated	Eth2/26, Eth2/27	200	202	community	Eth2/26, Eth2/28	<div>Example</div> <div><ul style="list-style-type: none">This command displays the private VLANs.</div> <div><pre>switch>show vlan private-vlan</pre><table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>5</td><td>25</td><td>isolated</td><td></td></tr><tr><td>5</td><td>26</td><td>isolated</td><td></td></tr><tr><td>7</td><td>31</td><td>community</td><td></td></tr><tr><td>7</td><td>32</td><td>isolated</td><td></td></tr></tbody></table><pre>switch></pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 790.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 637; Arista User Manual, v. 4.11.1 (1/11/13), at 491; Arista User Manual v. 4.10.3 (10/22/12), at 409; Arista User Manual v. 4.9.3.2 (5/3/12), at 344.</div>	Primary	Secondary	Type	Ports	5	25	isolated		5	26	isolated		7	31	community		7	32	isolated	
Primary	Secondary	Type	Ports																															
200	201	isolated	Eth2/26, Eth2/27																															
200	202	community	Eth2/26, Eth2/28																															
Primary	Secondary	Type	Ports																															
5	25	isolated																																
5	26	isolated																																
7	31	community																																
7	32	isolated																																

Copyright Registration Information	Cisco	Arista																																
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to display information about all private VLANs on the device:</p> <pre>switch(config)# show vlan private-vlan</pre> <table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>200</td><td>201</td><td>isolated</td><td>Eth2/26, Eth2/27</td></tr><tr><td>200</td><td>202</td><td>community</td><td>Eth2/26, Eth2/28</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2010), at L2-96</p>	Primary	Secondary	Type	Ports	200	201	isolated	Eth2/26, Eth2/27	200	202	community	Eth2/26, Eth2/28	<p>Example</p> <ul style="list-style-type: none">This command displays the private VLANs. <pre>switch>show vlan private-vlan</pre> <table><thead><tr><th>Primary</th><th>Secondary</th><th>Type</th><th>Ports</th></tr></thead><tbody><tr><td>5</td><td>25</td><td>isolated</td><td></td></tr><tr><td>5</td><td>26</td><td>isolated</td><td></td></tr><tr><td>7</td><td>31</td><td>community</td><td></td></tr><tr><td>7</td><td>32</td><td>isolated</td><td></td></tr></tbody></table> <p>switch></p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 790.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 637; Arista User Manual, v. 4.11.1 (1/11/13), at 491; Arista User Manual v. 4.10.3 (10/22/12), at 409; Arista User Manual v. 4.9.3.2 (5/3/12), at 344.</p>	Primary	Secondary	Type	Ports	5	25	isolated		5	26	isolated		7	31	community		7	32	isolated	
	Primary	Secondary	Type	Ports																														
200	201	isolated	Eth2/26, Eth2/27																															
200	202	community	Eth2/26, Eth2/28																															
Primary	Secondary	Type	Ports																															
5	25	isolated																																
5	26	isolated																																
7	31	community																																
7	32	isolated																																
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>spanning-tree bpdupfilter</p> <p>To enable bridge protocol data unit (BPDU) Filtering on the interface, use the spanning-tree bpdupfilter command. To return to the default settings, use the no form of this command.</p> <pre>spanning-tree bpdupfilter {enable disable}</pre> <p>no spanning-tree bpdupfilter</p> <table><thead><tr><th>Syntax</th><th>Description</th></tr></thead><tbody><tr><td>enable</td><td>Enables BPDU Filtering on this interface.</td></tr><tr><td>disable</td><td>Disables BPDU Filtering on this interface.</td></tr></tbody></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 111.</p>	Syntax	Description	enable	Enables BPDU Filtering on this interface.	disable	Disables BPDU Filtering on this interface.	<p>spanning-tree bpdupfilter</p> <p>The spanning-tree bpdupfilter command controls bridge protocol data unit (BPDU) filtering on the configuration mode interface. BPDU filtering is disabled by default.</p> <p>Ports with BPDU filtering enabled drop inbound BPDUs and do not send BPDUs. Enabling BPDU filtering on a port not connected to a host can result in loops as the port continues forwarding data while ignoring inbound BPDU packets.</p> <ul style="list-style-type: none">spanning-tree bpdupfilter enabled enables BPDU filtering.spanning-tree bpdupfilter disabled disables BPDU filtering by removing the spanning-tree bpdupfilter command from running-config. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 874; Arista User Manual, v. 4.11.1 (1/11/13), at 692; Arista User Manual v. 4.10.3 (10/22/12), at 606; Arista User Manual v. 4.9.3.2 (5/3/12), at 525; Arista User Manual v. 4.8.2 (11/18/11), at 399; Arista User Manual v. 4.7.3 (7/18/11), at 265.</p>																										
Syntax	Description																																	
enable	Enables BPDU Filtering on this interface.																																	
disable	Disables BPDU Filtering on this interface.																																	

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree bridge assurance</p> <p>To enable Bridge Assurance on the device, use the spanning-tree bridge assurance command. To disable Bridge Assurance, use the no form of this command.</p> <p>spanning-tree bridge assurance</p> <p>no spanning-tree bridge assurance</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 115.</p>	<p>spanning-tree bridge assurance</p> <p>The spanning-tree bridge assurance command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>The no spanning-tree bridge assurance command disables bridge assurance.</p> <p>The spanning-tree bridge assurance and default spanning-tree bridge assurance commands restore the default behavior by removing the no spanning-tree bridge assurance command from <i>running-config</i>. Only the no form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>spanning-tree bridge assurance</p> <p>no spanning-tree bridge assurance</p> <p>default spanning-tree bridge assurance</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree bridge assurance</p> <p>To enable Bridge Assurance on the device, use the spanning-tree bridge assurance command. To disable Bridge Assurance, use the no form of this command.</p> <p>spanning-tree bridge assurance</p> <p>no spanning-tree bridge assurance</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-106.</p>	<p>spanning-tree bridge assurance</p> <p>The spanning-tree bridge assurance command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>The no spanning-tree bridge assurance command disables bridge assurance.</p> <p>The spanning-tree bridge assurance and default spanning-tree bridge assurance commands restore the default behavior by removing the no spanning-tree bridge assurance command from <i>running-config</i>. Only the no form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>spanning-tree bridge assurance</p> <p>no spanning-tree bridge assurance</p> <p>default spanning-tree bridge assurance</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree bridge assurance</p> <p>To enable Bridge Assurance on the device, use the spanning-tree bridge assurance command. To disable Bridge Assurance, use the no form of this command.</p> <p>spanning-tree bridge assurance</p> <p>no spanning-tree bridge assurance</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-33.</p>	<p>spanning-tree bridge assurance</p> <p>The spanning-tree bridge assurance command enables bridge assurance on all ports with a port type of <i>network</i>. Bridge assurance protects against unidirectional link failure, other software failure, and devices that quit running a spanning tree algorithm.</p> <p>Bridge assurance is available only on spanning tree <i>network</i> ports on point-to-point links. Both ends of the link must have bridge assurance enabled. If the device on one side of the link has bridge assurance enabled and the device on the other side either does not support bridge assurance or does not have it enabled, the bridge assurance enabled port is blocked.</p> <p>The no spanning-tree bridge assurance command disables bridge assurance.</p> <p>The spanning-tree bridge assurance and default spanning-tree bridge assurance commands restore the default behavior by removing the no spanning-tree bridge assurance command from <i>running-config</i>. Only the no form of this command is visible in <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>spanning-tree bridge assurance no spanning-tree bridge assurance default spanning-tree bridge assurance</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 967.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 880; Arista User Manual, v. 4.11.1 (1/11/13), at 698; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 531; Arista User Manual v. 4.8.2 (11/18/11), at 403; Arista User Manual v. 4.7.3 (7/18/11), at 252.</p>

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree guard</p> <p>To enable or disable Loop Guard or Root Guard, use the spanning-tree guard command. To return to the default settings, use the no form of this command.</p> <p>spanning-tree guard {loop root none}</p> <p>no spanning-tree guard</p> <table border="1"> <tr> <td>Syntax Description</td><td>loop</td><td>Enables Loop Guard on the interface.</td></tr> <tr> <td></td><td>root</td><td>Enables Root Guard on the interface.</td></tr> <tr> <td></td><td>none</td><td>Sets the guard mode to none.</td></tr> </table> <p>Defaults Disabled</p> <p>Command Modes Interface configuration</p> <p>Supported User Roles network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines You cannot enable Loop Guard if Root Guard is enabled, although the device accepts the command to enable Loop Guard on spanning tree edge ports. This command does not require a license.</p> <p>Examples This example shows how to enable Root Guard: <pre>switch(config-if)# spanning-tree guard root switch(config-if)#</pre></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 119.</p>	Syntax Description	loop	Enables Loop Guard on the interface.		root	Enables Root Guard on the interface.		none	Sets the guard mode to none.	Command History	Release	Modification		4.0	This command was introduced.	<p>spanning-tree guard</p> <p>The spanning-tree guard command enables root guard or loop guard on the configuration mode interface. The spanning-tree loopguard default command configures the global loop guard setting.</p> <ul style="list-style-type: none"> Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Loop guard protects against loops resulting from unidirectional link failures on point-to-point links by preventing non-designated ports from becoming designated ports. When loop guard is enabled, a root or blocked port transitions to loop-inconsistent (blocked) state if it stops receiving BPDUs from its designated port. The port returns to its prior state when it receives a BPDU. <p>The no spanning-tree guard and default spanning-tree guard commands sets the configuration mode interface to the global loop guard mode by removing the spanning-tree guard statement from <i>running-config</i>. The spanning-tree guard none command disables loop guard and root guard on the interface, overriding the global setting.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration</p> <p>Command Syntax</p> <p>spanning-tree guard <i>PORT MODE</i> no spanning-tree guard default spanning-tree guard</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>PORT MODE</i> the port mode. Options include: <ul style="list-style-type: none"> loop enables loop guard on the interface. root enables root guard on the interface. none disables root guard and loop guard. <p>Examples</p> <ul style="list-style-type: none"> This command enables root guard on Ethernet 5 interface. <pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree guard root switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1005.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>
Syntax Description	loop	Enables Loop Guard on the interface.															
	root	Enables Root Guard on the interface.															
	none	Sets the guard mode to none.															
Command History	Release	Modification															
	4.0	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree guard</p> <p>To enable or disable Loop Guard or Root Guard, use the spanning-tree guard command. To return to the default settings, use the no form of this command.</p> <p>spanning-tree guard {loop root none}</p> <p>no spanning-tree guard</p> <table border="1"> <tr> <td>Syntax Description</td><td>loop</td><td>Enables Loop Guard on the interface.</td></tr> <tr> <td></td><td>root</td><td>Enables Root Guard on the interface.</td></tr> <tr> <td></td><td>none</td><td>Sets the guard mode to none.</td></tr> </table> <p>Defaults Disabled</p> <p>Command Modes Interface configuration</p> <p>SupportedUserRoles network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines You cannot enable Loop Guard if Root Guard is enabled, although the device accepts the command to enable Loop Guard on spanning tree edge ports. This command does not require a license.</p> <p>Examples This example shows how to enable Root Guard: <pre>switch(config-if)# spanning-tree guard root switch(config-if)#</pre></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L-110.</p>	Syntax Description	loop	Enables Loop Guard on the interface.		root	Enables Root Guard on the interface.		none	Sets the guard mode to none.	Command History	Release	Modification		4.0	This command was introduced.	<p>spanning-tree guard</p> <p>The spanning-tree guard command enables root guard or loop guard on the configuration mode interface. The spanning-tree loopguard default command configures the global loop guard setting.</p> <ul style="list-style-type: none"> Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Loop guard protects against loops resulting from unidirectional link failures on point-to-point links by preventing non-designated ports from becoming designated ports. When loop guard is enabled, a root or blocked port transitions to loop-inconsistent (blocked) state if it stops receiving BPDUs from its designated port. The port returns to its prior state when it receives a BPDU. <p>The no spanning-tree guard and default spanning-tree guard commands sets the configuration mode interface to the global loop guard mode by removing the spanning-tree guard statement from <i>running-config</i>. The spanning-tree guard none command disables loop guard and root guard on the interface, overriding the global setting.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration</p> <p>Command Syntax</p> <p>spanning-tree guard <i>PORT MODE</i> no spanning-tree guard default spanning-tree guard</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>PORT MODE</i> the port mode. Options include: <ul style="list-style-type: none"> loop enables loop guard on the interface. root enables root guard on the interface. none disables root guard and loop guard. <p>Examples</p> <ul style="list-style-type: none"> This command enables root guard on Ethernet 5 interface. <pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree guard root switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1005.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>
Syntax Description	loop	Enables Loop Guard on the interface.															
	root	Enables Root Guard on the interface.															
	none	Sets the guard mode to none.															
Command History	Release	Modification															
	4.0	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree guard</p> <p>To enable or disable Loop Guard or Root Guard, use the spanning-tree guard command. To return to the default settings, use the no form of this command.</p> <p>spanning-tree guard {loop root none}</p> <p>no spanning-tree guard</p> <table border="1"> <tr> <td>Syntax Description</td><td>loop</td><td>Enables Loop Guard on the interface.</td></tr> <tr> <td></td><td>root</td><td>Enables Root Guard on the interface.</td></tr> <tr> <td></td><td>none</td><td>Sets the guard mode to none.</td></tr> </table> <p>Defaults Disabled</p> <p>Command Modes Interface configuration</p> <p>SupportedUserRoles network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines You cannot enable Loop Guard if Root Guard is enabled, although the device accepts the command to enable Loop Guard on spanning tree edge ports. This command does not require a license.</p> <p>Examples This example shows how to enable Root Guard: <pre>switch(config-if)# spanning-tree guard root switch(config-if)#</pre></p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L-37.</p>	Syntax Description	loop	Enables Loop Guard on the interface.		root	Enables Root Guard on the interface.		none	Sets the guard mode to none.	Command History	Release	Modification		4.0	This command was introduced.	<p>spanning-tree guard</p> <p>The spanning-tree guard command enables root guard or loop guard on the configuration mode interface. The spanning-tree loopguard default command configures the global loop guard setting.</p> <ul style="list-style-type: none"> Root guard prevents a port from becoming a root or blocked port. A root guard port that receives a superior BPDU transitions to the root-inconsistent (blocked) state. Loop guard protects against loops resulting from unidirectional link failures on point-to-point links by preventing non-designated ports from becoming designated ports. When loop guard is enabled, a root or blocked port transitions to loop-inconsistent (blocked) state if it stops receiving BPDUs from its designated port. The port returns to its prior state when it receives a BPDU. <p>The no spanning-tree guard and default spanning-tree guard commands sets the configuration mode interface to the global loop guard mode by removing the spanning-tree guard statement from <i>running-config</i>. The spanning-tree guard none command disables loop guard and root guard on the interface, overriding the global setting.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Port-Channel Configuration</p> <p>Command Syntax</p> <p>spanning-tree guard <i>PORT MODE</i> no spanning-tree guard default spanning-tree guard</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>PORT MODE</i> the port mode. Options include: <ul style="list-style-type: none"> loop enables loop guard on the interface. root enables root guard on the interface. none disables root guard and loop guard. <p>Examples</p> <ul style="list-style-type: none"> This command enables root guard on Ethernet 5 interface. <pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree guard root switch(config-if-Et5)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1005.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 883; Arista User Manual, v. 4.11.1 (1/11/13), at 701; Arista User Manual v. 4.10.3 (10/22/12), at 615; Arista User Manual v. 4.9.3.2 (5/3/12), at 534; Arista User Manual v. 4.8.2 (11/18/11), at 406; Arista User Manual v. 4.7.3 (7/18/11), at 268.</p>
Syntax Description	loop	Enables Loop Guard on the interface.															
	root	Enables Root Guard on the interface.															
	none	Sets the guard mode to none.															
Command History	Release	Modification															
	4.0	This command was introduced.															

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 121.</p>	<ul style="list-style-type: none"> spanning-tree loopguard default command enables loop guard as a default on all switch ports. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-112.</p>	<ul style="list-style-type: none"> spanning-tree loopguard default command enables loop guard as a default on all switch ports. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-39.</p>	<ul style="list-style-type: none"> spanning-tree loopguard default command enables loop guard as a default on all switch ports. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 996.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 844; Arista User Manual, v. 4.11.1 (1/11/13), at 662; Arista User Manual v. 4.10.3 (10/22/12), 576; Arista User Manual v. 4.9.3.2 (5/3/12), at 496; Arista User Manual v. 4.8.2 (11/18/11), at 370; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree loopguard default</p> <p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>spanning-tree loopguard default</p> <p>no spanning-tree loopguard default</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), at 121.</p>	<p>spanning-tree loopguard default</p> <p>The spanning-tree loopguard default command configures the global loop guard setting as <i>enabled</i>. Ports not covered by a spanning-tree guard command use the global loop guard setting. Loop guard prevents blocked or root ports from becoming a designated port due to failures resulting in a unidirectional link. The spanning-tree guard interface configuration statement overrides the global setting for a specified interface. The default global loop guard setting is <i>disabled</i>.</p> <p>The no spanning-tree loopguard default and default spanning-tree loopguard default commands restore the global loop guard setting of <i>disabled</i> by removing the spanning-tree loopguard default command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>spanning-tree loopguard default</p> <p>no spanning-tree loopguard default</p> <p>default spanning-tree loopguard default</p> <p>Examples</p> <ul style="list-style-type: none"> This command enables loop guard as the default on all switch ports. <pre>switch(config)#spanning-tree loopguard default switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1008.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 886; Arista User Manual, v. 4.11.1 (1/11/13), at 704; Arista User Manual v. 4.10.3 (10/22/12), at 618; Arista User Manual v. 4.9.3.2 (5/3/12), at 537; Arista User Manual v. 4.8.2 (11/18/11), at 409; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree loopguard default</p> <p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>spanning-tree loopguard default</p> <p>no spanning-tree loopguard default</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-112.</p>	<p>spanning-tree loopguard default</p> <p>The spanning-tree loopguard default command configures the global loop guard setting as <i>enabled</i>. Ports not covered by a spanning-tree guard command use the global loop guard setting. Loop guard prevents blocked or root ports from becoming a designated port due to failures resulting in a unidirectional link. The spanning-tree guard interface configuration statement overrides the global setting for a specified interface. The default global loop guard setting is <i>disabled</i>.</p> <p>The no spanning-tree loopguard default and default spanning-tree loopguard default commands restore the global loop guard setting of <i>disabled</i> by removing the spanning-tree loopguard default command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>spanning-tree loopguard default</p> <p>no spanning-tree loopguard default</p> <p>default spanning-tree loopguard default</p> <p>Examples</p> <ul style="list-style-type: none"> This command enables loop guard as the default on all switch ports. <pre>switch(config)#spanning-tree loopguard default switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1008.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 886; Arista User Manual, v. 4.11.1 (1/11/13), at 704; Arista User Manual v. 4.10.3 (10/22/12), at 618; Arista User Manual v. 4.9.3.2 (5/3/12), at 537; Arista User Manual v. 4.8.2 (11/18/11), at 409; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>spanning-tree loopguard default</p> <p>To enable Loop Guard as a default on all ports of a given bridge, use the spanning-tree loopguard default command. To disable Loop Guard, use the no form of this command.</p> <p>spanning-tree loopguard default</p> <p>no spanning-tree loopguard default</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-39.</p>	<p>spanning-tree loopguard default</p> <p>The spanning-tree loopguard default command configures the global loop guard setting as <i>enabled</i>. Ports not covered by a spanning-tree guard command use the global loop guard setting. Loop guard prevents blocked or root ports from becoming a designated port due to failures resulting in a unidirectional link. The spanning-tree guard interface configuration statement overrides the global setting for a specified interface. The default global loop guard setting is <i>disabled</i>.</p> <p>The no spanning-tree loopguard default and default spanning-tree loopguard default commands restore the global loop guard setting of <i>disabled</i> by removing the spanning-tree loopguard default command from <i>running-config</i>.</p> <p>Platform all Command Mode Global Configuration</p> <p>Command Syntax</p> <p>spanning-tree loopguard default</p> <p>no spanning-tree loopguard default</p> <p>default spanning-tree loopguard default</p> <p>Examples</p> <ul style="list-style-type: none"> This command enables loop guard as the default on all switch ports. <pre>switch(config)#spanning-tree loopguard default switch(config)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1008.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 886; Arista User Manual, v. 4.11.1 (1/11/13), at 704; Arista User Manual v. 4.10.3 (10/22/12), at 618; Arista User Manual v. 4.9.3.2 (5/3/12), at 537; Arista User Manual v. 4.8.2 (11/18/11), at 409; Arista User Manual v. 4.7.3 (7/18/11), at 255.</p>

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>spanning-tree mst configuration</div> <p>To enter the Multiple Spanning Tree (MST) configuration submode, use the spanning-tree mst configuration command. To return to the default settings, use the no form of this command.</p> <div>spanning-tree mst configuration</div> <div>no spanning-tree mst configuration</div> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, (2013), , at 124.</p>	<div>spanning-tree mst configuration</div> <p>The spanning-tree mst configuration command places the switch in MST-configuration mode, which is the group change mode where MST region parameters are configured.</p> <p>Changes made in a group change mode are saved by leaving the mode through the exit command or by entering another configuration mode. To discard changes from the current edit session, leave the mode with the abort command.</p> <p>These commands are available in MST-configuration mode:</p> <ul style="list-style-type: none">• abort (mst-configuration mode)• exit (mst-configuration mode)• instance• name (mst-configuration mode)• revision (mst-configuration mode)• show (mst-configuration mode) <p>The no spanning-tree mst configuration and default spanning-tree mst configuration commands restore the MST default configuration.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <p>Command Syntax</p> <div>spanning-tree mst configuration</div> <div>no spanning-tree mst configuration</div> <div>default spanning-tree mst configuration</div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1012.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 890; Arista User Manual, v. 4.11.1 (1/11/13), at 708; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 541; Arista User Manual v. 4.8.2 (11/18/11), at 413.</p>	Platform	all	Command Mode	Global Configuration
	Platform	all				
Command Mode	Global Configuration					

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>spanning-tree mst configuration</div> <p>To enter the Multiple Spanning Tree (MST) configuration submode, use the spanning-tree mst configuration command. To return to the default settings, use the no form of this command.</p> <div>spanning-tree mst configuration</div> <div>no spanning-tree mst configuration</div> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-115.</p>	<div>spanning-tree mst configuration</div> <p>The spanning-tree mst configuration command places the switch in MST-configuration mode, which is the group change mode where MST region parameters are configured.</p> <p>Changes made in a group change mode are saved by leaving the mode through the exit command or by entering another configuration mode. To discard changes from the current edit session, leave the mode with the abort command.</p> <p>These commands are available in MST-configuration mode:</p> <ul style="list-style-type: none">• abort (mst-configuration mode)• exit (mst-configuration mode)• instance• name (mst-configuration mode)• revision (mst-configuration mode)• show (mst-configuration mode) <p>The no spanning-tree mst configuration and default spanning-tree mst configuration commands restore the MST default configuration.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <p>Command Syntax</p> <div>spanning-tree mst configuration</div> <div>no spanning-tree mst configuration</div> <div>default spanning-tree mst configuration</div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1012.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 890; Arista User Manual, v. 4.11.1 (1/11/13), at 708; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 541; Arista User Manual v. 4.8.2 (11/18/11), at 413.</p>	Platform	all	Command Mode	Global Configuration
	Platform	all				
Command Mode	Global Configuration					

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div>spanning-tree mst configuration</div> <p>To enter the Multiple Spanning Tree (MST) configuration submode, use the spanning-tree mst configuration command. To return to the default settings, use the no form of this command.</p> <div>spanning-tree mst configuration</div> <div>no spanning-tree mst configuration</div> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-42.</p>	<div>spanning-tree mst configuration</div> <p>The spanning-tree mst configuration command places the switch in MST-configuration mode, which is the group change mode where MST region parameters are configured.</p> <p>Changes made in a group change mode are saved by leaving the mode through the exit command or by entering another configuration mode. To discard changes from the current edit session, leave the mode with the abort command.</p> <p>These commands are available in MST-configuration mode:</p> <ul style="list-style-type: none">• abort (mst-configuration mode)• exit (mst-configuration mode)• instance• name (mst-configuration mode)• revision (mst-configuration mode)• show (mst-configuration mode) <p>The no spanning-tree mst configuration and default spanning-tree mst configuration commands restore the MST default configuration.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table> <p>Command Syntax</p> <div>spanning-tree mst configuration</div> <div>no spanning-tree mst configuration</div> <div>default spanning-tree mst configuration</div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1012.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 890; Arista User Manual, v. 4.11.1 (1/11/13), at 708; Arista User Manual v. 4.10.3 (10/22/12), at 612; Arista User Manual v. 4.9.3.2 (5/3/12), at 541; Arista User Manual v. 4.8.2 (11/18/11), at 413.</p>	Platform	all	Command Mode	Global Configuration
	Platform	all				
Command Mode	Global Configuration					

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 125.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-116.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-43.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															





Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS 15.1</p> <p>Effective date of registration: 11/28/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco IOS Configuration Fundamentals Command Reference (2010), at CF-488:CF-489.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															



Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS XE 2.1</p> <p>Effective date of registration: 11/24/2014</p>	<table border="1"> <thead> <tr> <th>Related Commands</th><th>Command</th><th>Description</th></tr> </thead> <tbody> <tr> <td></td><td><code>instance vlan</code></td><td>Maps a VLAN or a set of VLANs to an MST instance.</td></tr> <tr> <td></td><td><code>name (mst configuration)</code></td><td>Sets the name of an MST region.</td></tr> <tr> <td></td><td><code>revision</code></td><td>Sets the revision number for the MST configuration.</td></tr> <tr> <td></td><td><code>show spanning-tree mst</code></td><td>Displays information about the MST protocol.</td></tr> </tbody> </table> <p>Cisco IOS Configuration Fundamentals Command Reference (2008), at CF-466:CF467.</p>	Related Commands	Command	Description		<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.		<code>name (mst configuration)</code>	Sets the name of an MST region.		<code>revision</code>	Sets the revision number for the MST configuration.		<code>show spanning-tree mst</code>	Displays information about the MST protocol.	<p>The <code>instance</code> command inserts an entry into the VLAN-to-instance map that associates a set of VLANs to an MST instance. In addition to defining the MST topology, the VLAN-to-instance map is one of three parameters, along with the MST name and revision number, that identifies the switch's MST region.</p> <p>The <code>no instance</code> command removes specified entries from the VLAN-to-instance map. If the command does not provide a VLAN list, all entries are removed for the specified instance. The <code>no instance</code> and <code>default instance</code> commands function identically.</p> <p>Platform all Command Mode MST-Configuration</p> <p>Command Syntax</p> <pre>instance mst_inst vlans v_range no instance mst_inst [vlans v_range] no default instance mst_inst [vlans v_range]</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (October 2, 2014), at 978.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 856; Arista User Manual, v. 4.11.1 (1/11/13), at 674; Arista User Manual v. 4.10.3 (10/22/12), at 588; Arista User Manual v. 4.9.3.2 (5/3/12), at 507; Arista User Manual v. 4.8.2 (11/18/11), at 381; Arista User Manual v. 4.7.3 (7/18/11), at 293.</p>
Related Commands	Command	Description															
	<code>instance vlan</code>	Maps a VLAN or a set of VLANs to an MST instance.															
	<code>name (mst configuration)</code>	Sets the name of an MST region.															
	<code>revision</code>	Sets the revision number for the MST configuration.															
	<code>show spanning-tree mst</code>	Displays information about the MST protocol.															

Copyright Registration Information	Cisco	Arista																
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>show spanning-tree summary</td><td>Displays information about the spanning tree configuration.</td></tr><tr><td></td><td>spanning-tree bpduguard</td><td>Enables BPDU Guard on the interface.</td></tr><tr><td></td><td>spanning-tree port type edge</td><td>Configures an interface as a spanning tree edge port.</td></tr></table> <div>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 148.</div>	Related Commands	Command	Description		show spanning-tree summary	Displays information about the spanning tree configuration.		spanning-tree bpduguard	Enables BPDU Guard on the interface.		spanning-tree port type edge	Configures an interface as a spanning tree edge port.	<div>spanning-tree bpduguard</div> <div>The spanning-tree bpduguard command controls BPDU guard on the configuration mode interface. A BPDU guard-enabled port is disabled when it receives a BPDU packet. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</div> <div>The BPDU guard default setting for portfast ports is configured by the spanning-tree portfast bpduguard default command; BPDU guard is disabled by default on all non-portfast ports.</div> <div><ul style="list-style-type: none">spanning-tree bpduguard enable enables BPDU guard on the interface.spanning-tree bpduguard disable disables BPDU guard on the interface.</div> <div>The no spanning-tree bpduguard and default spanning-tree bpduguard commands restore the global BPDU guard setting on the configuration mode interface by removing the corresponding spanning-tree bpduguard command from running-config.</div> <div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration</td></tr></table></div> <div>Command Syntax</div> <div><pre>spanning-tree bpduguard <i>GUARD_ACTION</i> no spanning-tree bpduguard default spanning-tree bpduguard</pre></div> <div>Parameters</div> <div><ul style="list-style-type: none"><i>GUARD_ACTION</i> BPDU guard setting. Options include:<ul style="list-style-type: none">enabled BPDU guard is enabled on the interface.disabled BPDU guard is disabled on the interface.</div> <div>Examples</div> <div><ul style="list-style-type: none">These commands enable BPDU guard on Ethernet interface 5.<pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree bpduguard enabled switch(config-if-Et5)</pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 997.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 875; Arista User Manual, v. 4.11.1 (1/11/13), at 693; Arista User Manual v. 4.10.3 (10/22/12), at 607; Arista User Manual v. 4.9.3.2 (5/3/12), at 526; Arista User Manual v. 4.8.2 (11/18/11), at 400; Arista User Manual v. 4.7.3 (7/18/11), at 266.</div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration
	Related Commands	Command	Description															
		show spanning-tree summary	Displays information about the spanning tree configuration.															
	spanning-tree bpduguard	Enables BPDU Guard on the interface.																
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.																
Platform	all																	
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration																	

Copyright Registration Information	Cisco	Arista																
<div>Cisco NX-OS 5.0</div> <div>Effective date of registration: 11/13/2014</div>	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>show spanning-tree summary</td><td>Displays information about the spanning tree configuration.</td></tr><tr><td></td><td>spanning-tree bpduguard</td><td>Enables BPDU Guard on the interface.</td></tr><tr><td></td><td>spanning-tree port type edge</td><td>Configures an interface as a spanning tree edge port.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 5.x (2010), at L2-138.</p>	Related Commands	Command	Description		show spanning-tree summary	Displays information about the spanning tree configuration.		spanning-tree bpduguard	Enables BPDU Guard on the interface.		spanning-tree port type edge	Configures an interface as a spanning tree edge port.	<div><h3>spanning-tree bpduguard</h3><p>The spanning-tree bpduguard command controls BPDU guard on the configuration mode interface. A BPDU guard-enabled port is disabled when it receives a BPDU packet. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</p><p>The BPDU guard default setting for portfast ports is configured by the spanning-tree portfast bpduguard default command; BPDU guard is disabled by default on all non-portfast ports.</p><ul style="list-style-type: none">• spanning-tree bpduguard enable enables BPDU guard on the interface.• spanning-tree bpduguard disable disables BPDU guard on the interface.<p>The no spanning-tree bpduguard and default spanning-tree bpduguard commands restore the global BPDU guard setting on the configuration mode interface by removing the corresponding spanning-tree bpduguard command from <i>running-config</i>.</p><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration</td></tr></table><p>Command Syntax</p><pre>spanning-tree bpduguard <i>GUARD_ACTION</i> no spanning-tree bpduguard default spanning-tree bpduguard</pre><p>Parameters</p><ul style="list-style-type: none">• <i>GUARD_ACTION</i> BPDU guard setting. Options include:<ul style="list-style-type: none">— enabled BPDU guard is enabled on the interface.— disabled BPDU guard is disabled on the interface.<p>Examples</p><ul style="list-style-type: none">• These commands enable BPDU guard on Ethernet interface 5.<pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree bpduguard enabled switch(config-if-Et5)</pre><p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 997.</p><p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 875; Arista User Manual, v. 4.11.1 (1/11/13), at 693; Arista User Manual v. 4.10.3 (10/22/12), at 607; Arista User Manual v. 4.9.3.2 (5/3/12), at 526; Arista User Manual v. 4.8.2 (11/18/11), at 400; Arista User Manual v. 4.7.3 (7/18/11), at 266.</p></div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration
	Related Commands	Command	Description															
		show spanning-tree summary	Displays information about the spanning tree configuration.															
	spanning-tree bpduguard	Enables BPDU Guard on the interface.																
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.																
Platform	all																	
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration																	

Copyright Registration Information	Cisco	Arista																
<div>Cisco NX-OS 4.0</div> <div>Effective date of registration: 11/13/2014</div>	<table><tr><th>Related Commands</th><th>Command</th><th>Description</th></tr><tr><td></td><td>show spanning-tree summary</td><td>Displays information about the spanning tree configuration.</td></tr><tr><td></td><td>spanning-tree bpduguard</td><td>Enables BPDU Guard on the interface.</td></tr><tr><td></td><td>spanning-tree port type edge</td><td>Configures an interface as a spanning tree edge port.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-65.</p>	Related Commands	Command	Description		show spanning-tree summary	Displays information about the spanning tree configuration.		spanning-tree bpduguard	Enables BPDU Guard on the interface.		spanning-tree port type edge	Configures an interface as a spanning tree edge port.	<p>spanning-tree bpduguard</p> <p>The spanning-tree bpduguard command controls BPDU guard on the configuration mode interface. A BPDU guard-enabled port is disabled when it receives a BPDU packet. Disabled ports differ from blocked ports in that they are re-enabled only through manual intervention.</p> <p>The BPDU guard default setting for portfast ports is configured by the spanning-tree portfast bpduguard default command; BPDU guard is disabled by default on all non-portfast ports.</p> <ul style="list-style-type: none">• spanning-tree bpduguard enable enables BPDU guard on the interface.• spanning-tree bpduguard disable disables BPDU guard on the interface. <p>The no spanning-tree bpduguard and default spanning-tree bpduguard commands restore the global BPDU guard setting on the configuration mode interface by removing the corresponding spanning-tree bpduguard command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration</td></tr></table> <p>Command Syntax</p> <pre>spanning-tree bpduguard <i>GUARD_ACTION</i> no spanning-tree bpduguard default spanning-tree bpduguard</pre> <p>Parameters</p> <ul style="list-style-type: none">• <i>GUARD_ACTION</i> BPDU guard setting. Options include:<ul style="list-style-type: none">— enabled BPDU guard is enabled on the interface.— disabled BPDU guard is disabled on the interface. <p>Examples</p> <ul style="list-style-type: none">• These commands enable BPDU guard on Ethernet interface 5.<pre>switch(config)#interface ethernet 5 switch(config-if-Et5)#spanning-tree bpduguard enabled switch(config-if-Et5)</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 997.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 875; Arista User Manual, v. 4.11.1 (1/11/13), at 693; Arista User Manual v. 4.10.3 (10/22/12), at 607; Arista User Manual v. 4.9.3.2 (5/3/12), at 526; Arista User Manual v. 4.8.2 (11/18/11), at 400; Arista User Manual v. 4.7.3 (7/18/11), at 266.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration
	Related Commands	Command	Description															
	show spanning-tree summary	Displays information about the spanning tree configuration.																
	spanning-tree bpduguard	Enables BPDU Guard on the interface.																
	spanning-tree port type edge	Configures an interface as a spanning tree edge port.																
Platform	all																	
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration																	

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p> Caution When disabling spanning tree on a VLAN using the <code>no spanning-tree vlan <i>vlan-id</i></code> command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.</p> <p> Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.</p> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference (2013), at 159.</p>	<p>Warning Disabling spanning tree is not recommended, even in topologies free of physical loops. Spanning tree guards against configuration mistakes and cabling errors. When disabling VLAN, ensure that there are no physical loops in the VLAN.</p> <p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1023.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p> Caution When disabling spanning tree on a VLAN using the <code>no spanning-tree vlan <i>vlan-id</i></code> command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.</p> <p> Caution We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.</p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at L2-150.</p>	<p>Warning Disabling spanning tree is not recommended, even in topologies free of physical loops. Spanning tree guards against configuration mistakes and cabling errors. When disabling VLAN, ensure that there are no physical loops in the VLAN.</p> <p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1023.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="310 280 1134 418">  <p>When disabling spanning tree on a VLAN using the <code>no spanning-tree vlan <i>vlan-id</i></code> command, ensure that all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the same VLAN because switches and bridges with spanning tree enabled have incomplete information about the physical topology of the network.</p> </div> <div data-bbox="310 435 1134 535">  <p>We do not recommend disabling spanning tree even in a topology that is free of physical loops. Spanning tree is a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.</p> </div> <p>Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference, Release 4.x (2008), at L2-75.</p>	<div data-bbox="1182 280 2032 354"> <p>Warning Disabling spanning tree is not recommended, even in topologies free of physical loops. Spanning tree guards against configuration mistakes and cabling errors. When disabling VLAN, ensure that there are no physical loops in the VLAN.</p> </div> <div data-bbox="1182 386 2032 475"> <p>Important When disabling spanning tree on a VLAN, ensure that all switches and bridges in the network disable spanning tree for the same VLAN. Disabling spanning tree on a subset of switches and bridges in a VLAN may have unexpected results because switches and bridges running spanning tree will have incomplete information regarding the network's physical topology.</p> </div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1023.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 901; Arista User Manual, v. 4.11.1 (1/11/13), at 719; Arista User Manual v. 4.10.3 (10/22/12), at 633; Arista User Manual v. 4.9.3.2 (5/3/12), at 550; Arista User Manual v. 4.8.2 (11/18/11), at 422; Arista User Manual v. 4.7.3 (7/18/11), at 264.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>switchport private-vlan trunk native vlan</p> <p>To set the native VLAN for private VLAN promiscuous and isolated trunk ports, use the switchport private-vlan trunk native vlan command. To return to the default value, use the no form of this command.</p> <p>switchport private-vlan trunk native vlan <i>vlan-id</i></p> <p>no switchport private-vlan trunk native vlan <i>vlan-id</i></p> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), 177.</p>	<p>switchport trunk native vlan</p> <p>The switchport trunk native vlan command specifies the trunk mode native VLAN for the configuration mode interface. Interfaces in trunk mode associate untagged frames with the native VLAN. Trunk mode interfaces can also be configured to drop untagged frames. The default native VLAN for all interfaces is VLAN 1.</p> <p>The no switchport trunk native vlan and default switchport trunk native vlan commands restore VLAN 1 as the trunk mode native VLAN to the configuration mode interface by removing the corresponding switchport trunk native vlan command from <i>running-config</i>.</p> <p>Platform all Command Mode Interface-Ethernet Configuration Interface-Port-channel Configuration</p> <p>Command Syntax</p> <p>switchport trunk native vlan <i>VLAN ID</i> no switchport trunk native vlan default switchport trunk native vlan</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 800.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 647; Arista User Manual, v. 4.11.1 (1/11/13), at 500; Arista User Manual v. 4.10.3 (10/22/12), at 418; Arista User Manual v. 4.9.3.2 (5/3/12), at 357.</p>

Copyright Registration Information	Cisco	Arista												
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>switchport private-vlan trunk native vlan</div> <p>To set the native VLAN for private VLAN promiscuous and isolated trunk ports, use the switchport private-vlan trunk native vlan command. To return to the default value, use the no form of this command.</p> <div>switchport private-vlan trunk native vlan vlan-id</div> <div>no switchport private-vlan trunk native vlan vlan-id</div> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 5.x (2010), at L2-168.</p>	<div>switchport trunk native vlan</div> <p>The switchport trunk native vlan command specifies the trunk mode native VLAN for the configuration mode interface. Interfaces in trunk mode associate untagged frames with the native VLAN. Trunk mode interfaces can also be configured to drop untagged frames. The default native VLAN for all interfaces is VLAN 1.</p> <p>The no switchport trunk native vlan and default switchport trunk native vlan commands restore VLAN 1 as the trunk mode native VLAN to the configuration mode interface by removing the corresponding switchport trunk native vlan command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-channel Configuration</td></tr></table> <p>Command Syntax</p> <div>switchport trunk native vlan VLAN_ID</div> <div>no switchport trunk native vlan</div> <div>default switchport trunk native vlan</div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 800.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 647; Arista User Manual, v. 4.11.1 (1/11/13), at 500; Arista User Manual v. 4.10.3 (10/22/12), at 418; Arista User Manual v. 4.9.3.2 (5/3/12), at 357.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-channel Configuration								
	Platform	all												
Command Mode	Interface-Ethernet Configuration Interface-Port-channel Configuration													
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<table><tr><td>Syntax</td><td>Description</td></tr><tr><td>add</td><td>(Optional) Adds a VLAN to the current list.</td></tr><tr><td>except</td><td>(Optional) Specifies all VLANs except a particular VLAN.</td></tr><tr><td>none</td><td>(Optional) Specifies no VLANs.</td></tr><tr><td>remove</td><td>(Optional) Removes the VLANs from the current list.</td></tr><tr><td>vlan-id</td><td>VLAN ID. The range is from 2 to 1001.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Interfaces Command Reference, Release 6.x (2013), at 179.</p>	Syntax	Description	add	(Optional) Adds a VLAN to the current list.	except	(Optional) Specifies all VLANs except a particular VLAN.	none	(Optional) Specifies no VLANs.	remove	(Optional) Removes the VLANs from the current list.	vlan-id	VLAN ID. The range is from 2 to 1001.	<p>Parameters</p> <ul style="list-style-type: none">EDIT_ACTION modifications to the VLAN list.<ul style="list-style-type: none">v range Creates VLAN list from v range.add v range Adds specified VLANs to current list.all VLAN list contains all VLANs.except v range VLAN list contains all VLANs except those specified.none VLAN list is empty (no VLANs).remove v range Removes specified VLANs from current list. <p>Valid v range formats include number (1 to 4094), range, or comma-delimited list of numbers and ranges.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 751.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 599; Arista User Manual, v. 4.11.1 (1/11/13), at 480; Arista User Manual v. 4.10.3 (10/22/12), at 399; Arista User Manual v. 4.9.3.2 (5/3/12), at 355.</p>
Syntax	Description													
add	(Optional) Adds a VLAN to the current list.													
except	(Optional) Specifies all VLANs except a particular VLAN.													
none	(Optional) Specifies no VLANs.													
remove	(Optional) Removes the VLANs from the current list.													
vlan-id	VLAN ID. The range is from 2 to 1001.													

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>area stub (OSPF)</p> <p>To define an area as an Open Shortest Path First (OSPF) stub area, use the <code>area stub</code> command. To remove the area, use the <code>no</code> form of this command.</p> <pre>area area-id stub [no-summary] no area area-id stub [no-summary]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td><code>area-id</code></td><td>Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.</td></tr><tr><td><code>no-summary</code></td><td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 42.</p>	Syntax	Description	<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	<p>no area (OSPFv3)</p> <p>The <code>no area</code> command removes all area configuration commands for the specified OSPFv3 area. Commands removed by the <code>no area</code> command include:</p> <ul style="list-style-type: none">• <code>area</code>• <code>nssa</code>• <code>range</code>• <code>stub</code> <p>Area settings can be removed individually; refer to the command description page of the desired command for details.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>no area area_id [TYPE] default area area_id [TYPE]</pre> <p>Parameters</p> <ul style="list-style-type: none">• <code>area_id</code> area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.• <code>TYPE</code> area type. Values include:<ul style="list-style-type: none">— <code>nssa</code>— <code>nssa translate type7 always</code> sets p-bit when sending type 7 LSAs— <code>stub</code>— <code>stub no-summary</code> Prevents ABRs from sending summary link advertisements into the area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/24/2014), at 1521.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1305; Arista User Manual, v. 4.11.1 (1/11/13), at 1056; Arista User Manual v. 4.10.3 (10/22/12), at 781.</p>
	Syntax	Description						
	<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.						
<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>area stub (OSPF)</p> <p>To define an area as an Open Shortest Path First (OSPF) stub area, use the <code>area stub</code> command. To remove the area, use the <code>no</code> form of this command.</p> <pre>area area-id stub [no-summary] no area area-id stub [no-summary]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td>area-id</td><td>Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.</td></tr><tr><td>no-summary</td><td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-34.</p>	Syntax	Description	area-id	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	<p>no area (OSPFv3)</p> <p>The <code>no area</code> command removes all area configuration commands for the specified OSPFv3 area. Commands removed by the <code>no area</code> command include:</p> <ul style="list-style-type: none">• <code>area</code>• <code>nssa</code>• <code>range</code>• <code>stub</code> <p>Area settings can be removed individually; refer to the command description page of the desired command for details.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>no area area_id [TYPE] default area area_id [TYPE]</pre> <p>Parameters</p> <ul style="list-style-type: none">• <code>area_id</code> area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.• <code>TYPE</code> area type. Values include:<ul style="list-style-type: none">— <code>nssa</code>— <code>nssa translate type7 always</code> sets p-bit when sending type 7 LSAs— <code>stub</code>— <code>stub no-summary</code> Prevents ABRs from sending summary link advertisements into the area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/24/2014), at 1521.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1305; Arista User Manual, v. 4.11.1 (1/11/13), at 1056; Arista User Manual v. 4.10.3 (10/22/12), at 781.</p>
	Syntax	Description						
	area-id	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.						
no-summary	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<p>area stub (OSPF)</p> <p>To define an area as an Open Shortest Path First (OSPF) stub area, use the <code>area stub</code> command. To remove the area, use the <code>no</code> form of this command.</p> <pre>area area-id stub [no-summary] no area area-id stub [no-summary]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td><code>area-id</code></td><td>Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.</td></tr><tr><td><code>no-summary</code></td><td>(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-32.</p>	Syntax	Description	<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.	<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.	<p>no area (OSPFv3)</p> <p>The <code>no area</code> command removes all area configuration commands for the specified OSPFv3 area. Commands removed by the <code>no area</code> command include:</p> <ul style="list-style-type: none">• <code>area</code>• <code>nssa</code>• <code>range</code>• <code>stub</code> <p>Area settings can be removed individually; refer to the command description page of the desired command for details.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>no area area_id [TYPE] default area area_id [TYPE]</pre> <p>Parameters</p> <ul style="list-style-type: none">• <code>area_id</code> area number. Valid formats: integer <1 to 4294967295> or dotted decimal <0.0.0.1 to 255.255.255.255> Area 0 (or 0.0.0.0) is not configurable; it is always <i>normal</i>. <i>Running-config</i> stores value in dotted decimal notation.• <code>TYPE</code> area type. Values include:<ul style="list-style-type: none">— <code>nssa</code>— <code>nssa translate type7 always</code> sets p-bit when sending type 7 LSAs— <code>stub</code>— <code>stub no-summary</code> Prevents ABRs from sending summary link advertisements into the area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/24/2014), at 1521.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1305; Arista User Manual, v. 4.11.1 (1/11/13), at 1056; Arista User Manual v. 4.10.3 (10/22/12), at 781.</p>
	Syntax	Description						
	<code>area-id</code>	Identifier for the OSPF stub area. Specify as either a positive integer value or an IP address.						
<code>no-summary</code>	(Optional) Prevents an Area Border Router (ABR) from sending summary link advertisements into the stub area.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>This example shows how to clear all OSPF neighbor details for all OSPF instances:</p> <pre>switch# clear ip ospf neighbor *</pre> <p>This example shows how to clear all OSPF neighbor details for all neighbors on Ethernet interface 1/2 for OSPF instance 202:</p> <pre>switch# clear ip ospf 202 neighbor ethernet 1/2</pre> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 112.</p>	<p>Examples</p> <ul style="list-style-type: none">This command resets all OSPF neighbor statistics. <pre>switch#clear ip ospf neighbor * switch#</pre> <ul style="list-style-type: none">This command resets the OSPF neighbor statistics for the specified Ethernet 3 interface. <pre>switch#clear ip ospf neighbor ethernet 3 switch##</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1420.</p>						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>default-information originate (OSPF)</p> <p>To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</p> <pre>default-information originate [always] [route-map map-name] no default-information originate [always] [route-map map-name]</pre> <table><tr><th>Syntax</th><th>Description</th></tr><tr><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 42.</p>	Syntax	Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.	route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.	<p>Examples</p> <ul style="list-style-type: none">These commands will always advertise the OSPFv2 default route regardless of whether the switch has a default route configured. <pre>switch(config)#router ospf 1 switch((config-router-ospf)#default-information originate always switch(config-router-ospf)#show active router ospf 1 default-information originate always</pre> <ul style="list-style-type: none">These commands advertise a default route with a metric of 100 and an external metric type of 1 if a default route is configured. <pre>switch(config)#router ospf 1 switch((config-router-ospf)#default-information originate metric 100 metric-type 1</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1423.</p>
Syntax	Description							
always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.							
route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>default-information originate (OSPFv3)</div> <div>To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</div> <div>default-information originate [always] [route-map map-name] no default-information originate [always] [route-map map-name]</div> <div><table><tr><td>Syntax Description</td><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td></td><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.</td></tr></table></div> <div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 44.</div>	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.		route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.	<div>Examples</div> <div><ul style="list-style-type: none">These commands will always advertise the OSPFv3 default route regardless of whether the switch has a default route configured.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate always switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate always</pre>These commands configures OSPF area 1 as metric of 100 for the default route with an external metric type of Type 1.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#</pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1506.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1291; Arista User Manual, v. 4.11.1 (1/11/13), at 1041.</div>
	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.					
	route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.						

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>default-information originate (OSPFv3)</div> <div>To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) routing domain, use the default-information originate command. To disable this feature, use the no form of this command.</div> <div>default-information originate [always] [route-map map-name]</div> <div>no default-information originate [always] [route-map map-name]</div> <div><table><tr><td>Syntax Description</td><td>always</td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td></td><td>route-map map-name</td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.</td></tr></table></div>	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.		route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.	<div>Examples</div> <div><ul style="list-style-type: none">These commands will always advertise the OSPFv3 default route regardless of whether the switch has a default route configured.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate always switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate always</pre>These commands configures OSPF area 1 as metric of 100 for the default route with an external metric type of Type 1.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#</pre></div>
	Syntax Description	always	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.					
	route-map map-name	(Optional) Specifies to advertise the default route if the route map is satisfied. The map-name argument can be any alphanumeric string up to 63 characters.						
Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-155.	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1506. See also Arista User Manual v. 4.12.3 (7/17/13), at 1291; Arista User Manual, v. 4.11.1 (1/11/13), at 1041.							

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<h3>default-information originate (OSPFv3)</h3> <p>To generate a default external route into an Open Shortest Path First version 3 (OSPFv3) routing domain, use the <code>default-information originate</code> command. To disable this feature, use the <code>no</code> form of this command.</p> <pre>default-information originate [always] [route-map map-name] no default-information originate [always] [route-map map-name]</pre> <table><tr><th>Syntax Description</th><td><code>always</code></td><td>(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.</td></tr><tr><td></td><td><code>route-map map-name</code></td><td>(Optional) Specifies to advertise the default route if the route map is satisfied. The <code>map-name</code> argument can be any alphanumeric string up to 63 characters.</td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-90.</p>	Syntax Description	<code>always</code>	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.		<code>route-map map-name</code>	(Optional) Specifies to advertise the default route if the route map is satisfied. The <code>map-name</code> argument can be any alphanumeric string up to 63 characters.	<h3>Examples</h3> <ul style="list-style-type: none">These commands will always advertise the OSPFv3 default route regardless of whether the switch has a default route configured.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate always switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate always</pre>These commands configures OSPF area 1 as metric of 100 for the default route with an external metric type of Type 1.<pre>switch(config)#ipv6 router ospf 1 switch(config-router-ospf3)#default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#show active ipv6 router ospf 1 default-information originate metric 100 metric-type 1 switch(config-router-ospf3)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1506.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1291; Arista User Manual, v. 4.11.1 (1/11/13), at 1041.</p>
	Syntax Description	<code>always</code>	(Optional) Specifies to always advertise the default route regardless of whether the route table has a default route.					
		<code>route-map map-name</code>	(Optional) Specifies to advertise the default route if the route map is satisfied. The <code>map-name</code> argument can be any alphanumeric string up to 63 characters.					

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div>distance (EIGRP)</div><div><p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the distance command. To reset to default, use the no form of this command.</p><div><div>distance</div><div>internal-distance external-distance</div></div><div><div>no distance</div></div></div><div><div><div>Syntax Description</div><div><div><div>internal-distance</div><div>Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</div></div><div><div>external-distance</div><div>Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</div></div></div><div><div>Defaults</div><div><div>internal-distance: 90</div><div>external-distance: 170</div></div></div></div><div><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 61.</div></div></div></div>	<div><div>distance bgp</div><div><p>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p><p>The distance command assigns distance values to external, internal, and local BGP routes:</p><ul style="list-style-type: none"><div><div>external</div><div>External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.</div></div><div><div>internal</div><div>Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.</div></div><div><div>local</div><div>Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.</div></div><p>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from running-config.</p><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Router-BGP Configuration</div></div><div><div>Command Syntax</div><div><div>distance bgp external_dist [INTERNAL_LOCAL]</div><div>no distance bgp</div><div>default distance bgp</div></div><div><div>Parameters</div><ul style="list-style-type: none"><div><div>external_dist</div><div>distance assigned to external routes. Values range from 1 to 255.</div></div><div><div>INTERNAL_LOCAL</div><div>distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:</div><div><div><no parameter></div><div>external_dist value is assigned to internal and local routes.</div><div>internal_dist local_dist values assigned to internal (internal_dist) and local (local_dist) routes.</div></div></div></div></div><div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</div><div><div>See also</div><div>Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</div></div></div></div></div>

Copyright Registration Information	Cisco	Arista						
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<p>distance (EIGRP)</p> <p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the <code>distance</code> command. To reset to default, use the <code>no</code> form of this command.</p> <p><code>distance</code> <i>internal-distance external-distance</i></p> <p><code>no distance</code></p> <table><tr><td>Syntax Description</td><td><i>internal-distance</i></td><td>Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</td></tr><tr><td></td><td><i>external-distance</i></td><td>Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</td></tr></table> <p>Defaults</p> <p><i>internal-distance</i>: 90 <i>external-distance</i>: 170</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-171.</p>	Syntax Description	<i>internal-distance</i>	Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.		<i>external-distance</i>	Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.	<p>distance bgp</p> <p>The <code>distance bgp</code> command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p> <p>The distance command assigns distance values to external, internal, and local BGP routes:</p> <ul style="list-style-type: none">external: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.internal: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.local: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200. <p>The <code>no distance bgp</code> and <code>default distance bgp</code> commands restore the default administrative distances by removing the <code>distance bgp</code> command from <i>running-config</i>.</p> <p>Platform all Command Mode Router-BGP Configuration</p> <p>Command Syntax</p> <p><code>distance bgp external_dist [INTERNAL_LOCAL]</code> <code>no distance bgp</code> <code>default distance bgp</code></p> <p>Parameters</p> <ul style="list-style-type: none"><i>external_dist</i> distance assigned to external routes. Values range from 1 to 255.<i>INTERNAL_LOCAL</i> distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:<ul style="list-style-type: none"><code><no parameter></code> <i>external_dist</i> value is assigned to internal and local routes.<i>internal_dist local_dist</i> values assigned to internal (<i>internal_dist</i>) and local (<i>local_dist</i>) routes. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</p>
	Syntax Description	<i>internal-distance</i>	Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.					
	<i>external-distance</i>	Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.						

Copyright Registration Information	Cisco	Arista			
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div><div>distance (EIGRP)</div><div><p>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the <code>distance</code> command. To reset to default, use the <code>no</code> form of this command.</p><div><div>distance</div><div>internal-distance external-distance</div></div><div><div>no distance</div></div></div><div><table><tr><td>Syntax Description</td><td><div><div>internal-distance</div><div>Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</div></div></td><td><div><div>external-distance</div><div>Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</div></div></td></tr></table><div><div>Defaults</div><div><div>internal-distance: 90</div><div>external-distance: 170</div></div></div><div><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-104.</div></div></div></div>	Syntax Description	<div><div>internal-distance</div><div>Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</div></div>	<div><div>external-distance</div><div>Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</div></div>	<div><div>distance bgp</div><div><p>The distance <code>bgp</code> command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</p><p>The distance command assigns distance values to external, internal, and local BGP routes:</p><ul style="list-style-type: none"><div><div>external</div><div>External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.</div></div><div><div>internal</div><div>Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.</div></div><div><div>local</div><div>Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.</div></div><p>The <code>no distance bgp</code> and <code>default distance bgp</code> commands restore the default administrative distances by removing the <code>distance bgp</code> command from <i>running-config</i>.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-BGP Configuration</div></div><div><div>Command Syntax</div><div><div>distance bgp</div><div>external_dist [INTERNAL_LOCAL]</div><div>no distance bgp</div><div>default distance bgp</div></div></div><div><div>Parameters</div><ul style="list-style-type: none"><div><div>external_dist</div><div>distance assigned to external routes. Values range from 1 to 255.</div></div><div><div>INTERNAL_LOCAL</div><div>distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:</div><div><div><div><no parameter></div><div>external_dist value is assigned to internal and local routes.</div></div><div><div>internal_dist local_dist</div><div>values assigned to internal (internal_dist) and local (local_dist) routes.</div></div></div></div></div><div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</div><div><div>See also</div><div>Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</div></div></div></div></div>
	Syntax Description	<div><div>internal-distance</div><div>Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</div></div>	<div><div>external-distance</div><div>Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</div></div>		

Copyright Registration Information	Cisco	Arista						
Cisco IOS 15.0 Effective date of registration: 11/28/2014	<div>distance (EIGRP)</div> <div>To allow the use of two administrative distances—internal and external—for the Enhanced Interior Gateway Routing Protocol (EIGRP) that could provide a better route to a node, use the distance command. To reset to default, use the no form of this command.</div> <div><div>distance</div> internal-distance external-distance</div> <div><div>no distance</div></div> <div><table><tr><td>Syntax Description</td><td>internal-distance</td><td>Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.</td></tr><tr><td></td><td>external-distance</td><td>Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.</td></tr></table></div> <div><div>Defaults</div><div>internal-distance: 90 external-distance: 170</div></div> <div>Cisco IOS IP Routing: EIGRP Command Reference (2009), at IRE-33.</div>	Syntax Description	internal-distance	Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.		external-distance	Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.	<div>distance bgp</div> <div>The distance bgp command assigns an administrative distance to routes that the switch learns through BGP. Routers use administrative distances to select a route when two protocols provide routing information to the same destination. Distance values range from 1 to 255; lower distance values correspond to higher reliability. BGP routing tables do not include routes with a distance of 255.</div> <div>The distance command assigns distance values to external, internal, and local BGP routes:</div> <div><ul style="list-style-type: none"><div>external</div>: External routes are routes for which the best path is learned from a neighbor external to the autonomous system. Default distance is 200.<div>internal</div>: Internal routes are routes learned from a BGP entity within the same autonomous system. Default distance is 200.<div>local</div>: Local routes are networks listed with a network router configuration command for that router or for networks that are redistributed from another process. Default distance is 200.</div> <div>The no distance bgp and default distance bgp commands restore the default administrative distances by removing the distance bgp command from running-config.</div> <div><div>Platform</div>all</div> <div><div>Command Mode</div>Router-BGP Configuration</div> <div>Command Syntax</div> <div><div>distance bgp</div> external_dist [INTERNAL_LOCAL]</div> <div><div>no distance</div> bgp</div> <div><div>default distance</div> bgp</div> <div>Parameters</div> <div><ul style="list-style-type: none"><div>external_dist</div> distance assigned to external routes. Values range from 1 to 255.<div>INTERNAL_LOCAL</div> distance assigned to internal and local routes. Values for both routes range from 1 to 255. Options include:<ul style="list-style-type: none"><div><no parameter></div> external_dist value is assigned to internal and local routes.<div>internal_dist local_dist</div> values assigned to internal (internal_dist) and local (local_dist) routes.</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1583.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1360; Arista User Manual, v. 4.11.1 (1/11/13), at 1106; Arista User Manual v. 4.10.3 (10/22/12), at 918; Arista User Manual v. 4.9.3.2 (5/3/12), at 684; Arista User Manual v. 4.8.2 (11/18/11), at 514; Arista User Manual v. 4.7.3 (7/18/11), at 379.</div>
	Syntax Description	internal-distance	Administrative distance for EIGRP internal routes. Internal routes are routes that are learned from another entity within the same autonomous system (AS). The distance can be a value from 1 to 255. The default value is 90.					
	external-distance	Administrative distance for EIGRP external routes. External routes are routes for which the best path is learned from a source external to this autonomous system. The distance can be a value from 1 to 255. The default value is 170.						

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>When you configure the <code>ip</code> command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 256.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that map an IP address to a corresponding MAC address. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>When you configure the <code>ip</code> command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-236.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that map an IP address to a corresponding MAC address. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>When you configure the <code>ip</code> command on an interface, the handling of proxy Address Resolution Protocol (ARP) requests changes (unless proxy ARP was disabled). Hosts send ARP requests to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP requests on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-143.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that map an IP address to a corresponding MAC address. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>Address Resolution Protocol (ARP) is an Internet protocol used to map an IP address to a MAC address. ARP finds the MAC address, also known as the hardware address, of an IP-routed host from its known IP address and maintains this mapping information in a table. The router uses this IP address and MAC address mapping information to send IP packets to the next-hop router in the network.</p> <p>Cisco IOS IP Addressing Services Configuration Guide (2009), at CSI-CLI-00061623.</p>	<p>Displaying ARP Entries</p> <p>The <code>show ip arp</code> command displays ARP cache entries that map an IP address to a corresponding MAC address. The table displays addresses by their host names when the command includes the <code>resolve</code> argument.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1225.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1038; Arista User Manual, v. 4.11.1 (1/11/13), at 840; Arista User Manual v. 4.10.3 (10/22/12), at 687.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 274.</p>	<p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 107.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>Expanded Community Lists</p> <p>Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first.</p> <p>Cisco IOS IP Routing: BGP Command Reference, (2009), at 274.</p>	<p>The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it matches the earliest part first.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 107.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 105; Arista User Manual, v. 4.11.1 (1/11/13), at 65; Arista User Manual v. 4.12.3 (7/17/13), at 95; Arista User Manual v. 4.10.3 (10/22/12), at 57; Arista User Manual v. 4.9.3.2 (5/3/12), at 53; Arista User Manual v. 4.8.2 (11/18/11), at 49.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precedence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 337.</p>	<p>Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2/2014), at 1226.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Static routes have a default administrative distance of 1. If you want a dynamic routing protocol to take precedence over a static route, you must configure the static route preference argument to be greater than the administrative distance of the dynamic routing protocol. For example, routes derived with Enhanced Interior Gateway Routing Protocol (EIGRP) have a default administrative distance of 100. To have a static route that would be overridden by an EIGRP dynamic route, specify an administrative distance greater than 100.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-311.</p>	<p>Static routes have a default administrative distance of 1. Assigning a higher administrative distance to a static route configures it to be overridden by dynamic routing data. For example, a static route with a distance value of 200 is overridden by OSPF intra-area routes with a default distance of 110.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2/2014), at 1226.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1082; Arista User Manual, v. 4.11.1 (1/11/13), at 860; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command. To reset the default value, use the no form of this command.</p> <p>is-type [level-1 level-1-2 level-2]</p> <p>no is-type [level-1 level-1-2 level-2]</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 407.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type LAYER_VALUE</p> <p>Parameters</p> <ul style="list-style-type: none"> LAYER_VALUE layer value. Options include: <ul style="list-style-type: none"> level-1 The switch operates as a Level-1 (intra-area) router. level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command. To reset the default value, use the no form of this command.</p> <p>is-type [level-1 level-1-2 level-2]</p> <p>no is-type [level-1 level-1-2 level-2]</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-373.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type LAYER_VALUE</p> <p>Parameters</p> <ul style="list-style-type: none"> LAYER_VALUE layer value. Options include: <ul style="list-style-type: none"> level-1 The switch operates as a Level-1 (intra-area) router. level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command. To reset the default value, use the no form of this command.</p> <p>is-type [level-1 level-1-2 level-2]</p> <p>no is-type [level-1 level-1-2 level-2]</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-208.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type LAYER_VALUE</p> <p>Parameters</p> <ul style="list-style-type: none"> LAYER_VALUE layer value. Options include: <ul style="list-style-type: none"> level-1 The switch operates as a Level-1 (intra-area) router. level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>is-type</p> <p>To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the is-type command in router configuration mode. To reset the default value, use the no form of this command.</p> <p>is-type [level-1 level-1-2 level-2 only]</p> <p>no is-type [level-1 level-1-2 level-2-only]</p> <p>Cisco IOS IP Routing: ISIS Command Reference (2009), at IRS-73.</p>	<p>is-type</p> <p>The is-type command configures the routing level for an instance of the IS-IS routing instance.</p> <p>Platform all Command Mode Router-IS-IS Configuration</p> <p>Command Syntax is-type LAYER_VALUE</p> <p>Parameters</p> <ul style="list-style-type: none"> LAYER_VALUE layer value. Options include: <ul style="list-style-type: none"> level-1 The switch operates as a Level-1 (intra-area) router. level-2 The switch operates as a Level-2 (inter-area) router. <p>Example</p> <ul style="list-style-type: none"> These commands configure Level 2 routing on interface Ethernet 5. <pre>switch(config)#router isis Osiris switch(config-router-isis)#is-type level-2 switch(config-router-isis)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1691.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1451.</p>

Copyright Registration Information	Cisco	Arista													
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>isis hello-multiplier</div> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <div>isis hello-multiplier multiplier {level-1 level-2}</div> <div>no isis hello-multiplier {level-1 level-2}</div> <table><tr><td>Syntax Description</td><td>multiplier</td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr><tr><td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr><tr><td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr></table> <div>Command Default</div> <p>The default settings are as follows:</p> <ul style="list-style-type: none">multiplier: 3Level 1 and Level 2 <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 423.</p>	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<div>isis hello-multiplier</div> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from running-config.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table> <div>Command Syntax</div> <div>isis hello-multiplier factor</div> <div>no isis hello-multiplier</div> <div>default isis hello-multiplier</div> <div>Parameters</div> <ul style="list-style-type: none">factor hello multiplier. Values range from 3 to 100; default is 3 <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	multiplier	Integer value. Range: 3 to 1000. Default: 3.												
	level-1	Configures the hello multiplier independently for Level 1 adjacencies.													
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.													
Platform	all														
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration														

Copyright Registration Information	Cisco	Arista									
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis hello-multiplier</p> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <p>isis hello-multiplier multiplier [level-1 level-2]</p> <p>no isis hello-multiplier [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>multiplier</i></td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr> <tr> <td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr> <tr> <td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr> </table> <p>Command Default The default settings are as follows:</p> <ul style="list-style-type: none"> <i>multiplier</i>: 3 Level 1 and Level 2 <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-389.</p>	Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<p>isis hello-multiplier</p> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from <i>running-config</i>.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis hello-multiplier factor</p> <p>no isis hello-multiplier</p> <p>default isis hello-multiplier</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>factor</i> hello multiplier. Values range from 3 to 100; default is 3 <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>
Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.									
	level-1	Configures the hello multiplier independently for Level 1 adjacencies.									
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.									

Copyright Registration Information	Cisco	Arista									
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis hello-multiplier</p> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <p>isis hello-multiplier multiplier [level-1 level-2]</p> <p>no isis hello-multiplier [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>multiplier</i></td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr> <tr> <td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr> <tr> <td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr> </table> <p>Command Default The default settings are as follows:</p> <ul style="list-style-type: none"> <i>multiplier</i>: 3 Level 1 and Level 2 <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2008), at L3-224.</p>	Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<p>isis hello-multiplier</p> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from <i>running-config</i>.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis hello-multiplier factor no isis hello-multiplier default isis hello-multiplier</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>factor</i> hello multiplier. Values range from 3 to 100; default is 3 <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>
Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.									
	level-1	Configures the hello multiplier independently for Level 1 adjacencies.									
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.									

Copyright Registration Information	Cisco	Arista									
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>isis hello-multiplier</p> <p>To specify the number of Intermediate System-to-Intermediate System (IS-IS) hello packets a neighbor must miss before the router should declare the adjacency as down, use the isis hello-multiplier command. To restore the default value, use the no form of this command.</p> <p>isis hello-multiplier multiplier [level-1 level-2]</p> <p>no isis hello-multiplier [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>multiplier</i></td><td>Integer value. Range: 3 to 1000. Default: 3.</td></tr> <tr> <td></td><td>level-1</td><td>Configures the hello multiplier independently for Level 1 adjacencies.</td></tr> <tr> <td></td><td>level-2</td><td>Configures the hello multiplier independently for Level 2 adjacencies.</td></tr> </table> <p>Command Default The default settings are as follows:</p> <ul style="list-style-type: none"> <i>multiplier</i>: 3 Level 1 and Level 2 <p>Cisco IOS IP Routing: ISIS Command Reference (2009), at IRS-54.</p>	Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.		level-1	Configures the hello multiplier independently for Level 1 adjacencies.		level-2	Configures the hello multiplier independently for Level 2 adjacencies.	<p>isis hello-multiplier</p> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from <i>running-config</i>.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis hello-multiplier factor no isis hello-multiplier default isis hello-multiplier</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>factor</i> hello multiplier. Values range from 3 to 100; default is 3 <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>
Syntax Description	<i>multiplier</i>	Integer value. Range: 3 to 1000. Default: 3.									
	level-1	Configures the hello multiplier independently for Level 1 adjacencies.									
	level-2	Configures the hello multiplier independently for Level 2 adjacencies.									

Copyright Registration Information	Cisco	Arista																											
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>isis priority</div> <p>To configure the priority of designated routers, use the <code>isis priority</code> command in interface configuration mode. To reset the default priority, use the <code>no</code> form of this command.</p> <div>isis priority number-value [level-1 level-2]</div> <div>no isis priority [level-1 level-2]</div> <table><tr><td>Syntax Description</td><td>number-value</td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr><tr><td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr><tr><td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr></table> <table><tr><td>Defaults</td><td>Priority of 64 Level 1 and Level 2</td></tr></table> <table><tr><td>Command Modes</td><td>Interface configuration</td></tr></table> <table><tr><td>SupportedUserRoles</td><td>network-admin vdc-admin</td></tr></table> <table><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></td></tr></table> <table><tr><td>Usage Guidelines</td><td><p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the <code>level-1</code> or <code>level-2</code> keyword resets priority only for Level 1 or Level 2 routing, respectively.</p><p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p><p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p><p>This command requires the Enterprise Services license.</p></td></tr></table> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 433.</p>	Syntax Description	number-value	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Defaults	Priority of 64 Level 1 and Level 2	Command Modes	Interface configuration	SupportedUserRoles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.	Usage Guidelines	<p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the <code>level-1</code> or <code>level-2</code> keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p>	<div>isis priority</div> <p>The <code>isis priority</code> command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The <code>no isis priority</code> and default <code>isis priority</code> commands restore the default priority (64) on the configuration mode interface.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table> <p>Command Syntax</p> <div>isis priority priority_level</div> <div>no isis priority</div> <div>default isis priority</div> <p>Parameters</p> <ul style="list-style-type: none">priority_level priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Syntax Description	number-value	Priority of a router and is a number from 0 to 127. The default value is 64.																										
	level-1	(Optional) Sets the priority for Level 1 independently.																											
	level-2	(Optional) Sets the priority for Level 2 independently.																											
Defaults	Priority of 64 Level 1 and Level 2																												
Command Modes	Interface configuration																												
SupportedUserRoles	network-admin vdc-admin																												
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.																								
Release	Modification																												
4.0(1)	This command was introduced.																												
Usage Guidelines	<p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the <code>level-1</code> or <code>level-2</code> keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p>																												
Platform	all																												
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration																												

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [level-1 level-2]</p> <p>no isis priority [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the level-1 or level-2 keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-397.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	level-1	(Optional) Sets the priority for Level 1 independently.															
	level-2	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [level-1 level-2]</p> <p>no isis priority [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the level-1 or level-2 keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-232.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	level-1	(Optional) Sets the priority for Level 1 independently.															
	level-2	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista															
<p>Cisco IOS 15.0</p> <p>Effective date of registration: 11/28/2014</p>	<p>isis priority</p> <p>To configure the priority of designated routers, use the isis priority command in interface configuration mode. To reset the default priority, use the no form of this command.</p> <p>isis priority <i>number-value</i> [level-1 level-2]</p> <p>no isis priority [level-1 level-2]</p> <table border="1"> <tr> <td>Syntax Description</td><td><i>number-value</i></td><td>Priority of a router and is a number from 0 to 127. The default value is 64.</td></tr> <tr> <td></td><td>level-1</td><td>(Optional) Sets the priority for Level 1 independently.</td></tr> <tr> <td></td><td>level-2</td><td>(Optional) Sets the priority for Level 2 independently.</td></tr> </table> <p>Defaults</p> <p>Priority of 64 Level 1 and Level 2</p> <p>Command Modes</p> <p>Interface configuration</p> <p>Supported User Roles</p> <p>network-admin vdc-admin</p> <table border="1"> <tr> <td>Command History</td><td>Release</td><td>Modification</td></tr> <tr> <td></td><td>4.0(1)</td><td>This command was introduced.</td></tr> </table> <p>Usage Guidelines</p> <p>Priorities can be configured for Level 1 and Level 2 independently. Specifying the level-1 or level-2 keyword resets priority only for Level 1 or Level 2 routing, respectively.</p> <p>The priority is used to determine which router on a LAN will be the designated router or Designated Intermediate System (DIS). The priorities are advertised in the hello packets. The router with the highest priority will become the DIS.</p> <p>In Intermediate System-to-Intermediate System (IS-IS), there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a router with a higher priority comes on line, it will take over the role from the current DIS. In the case of equal priorities, the highest MAC address breaks the tie.</p> <p>This command requires the Enterprise Services license.</p> <p>Cisco IOS IP Routing: ISIS Command Reference (2009), at IRS-63.</p>	Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.		level-1	(Optional) Sets the priority for Level 1 independently.		level-2	(Optional) Sets the priority for Level 2 independently.	Command History	Release	Modification		4.0(1)	This command was introduced.	<p>isis priority</p> <p>The isis priority command configures IS-IS router priority for the configuration mode interface.</p> <p>The priority is used to determine which device will be the Designated Intermediate System (DIS). The device with the highest priority will become the DIS.</p> <p>In IS-IS, there is no backup designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If a device with a higher priority comes on line, it will take over the role from the current DIS.</p> <p>The no isis priority and default isis priority commands restore the default priority (64) on the configuration mode interface.</p> <p>Platform all</p> <p>Command Mode Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</p> <p>Command Syntax</p> <p>isis priority <i>priority_level</i></p> <p>no isis priority</p> <p>default isis priority</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>priority_level</i> priority level. Value ranges from 0 to 127. Default value is 64. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1690.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1450.</p>
Syntax Description	<i>number-value</i>	Priority of a router and is a number from 0 to 127. The default value is 64.															
	level-1	(Optional) Sets the priority for Level 1 independently.															
	level-2	(Optional) Sets the priority for Level 2 independently.															
Command History	Release	Modification															
	4.0(1)	This command was introduced.															

Copyright Registration Information	Cisco	Arista										
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>log-adjacency-changes (IS-IS)</div> <p>To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the log-adjacency-changes configuration mode command. To disable this function, use the no form of this command.</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>This command is enabled by default.</div></div> <div><div>Command Modes</div><div>Router configuration VRF configuration</div></div> <div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div> <div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div> <div><div>Usage Guidelines</div><div>The log-adjacency-changes command is on by default but only up/down (full/down) events are reported.</div></div> <div><div>Examples</div><div>This example configures the router to send a syslog message when an IS-IS neighbor state changes: switch(config)# router isis switch(config-router)# log-adjacency-changes</div></div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.	<div>log-adjacency-changes (IS-IS)</div> <p>The log-adjacency-changes command configures the switch to send syslog messages either when it detects IS-IS link state changes or when it detects that a neighbor has gone up or down. Log message sending is disabled by default.</p> <p>The default option is active when running-config does not contain any form of the command. Entering the command in any form replaces the previous command state in running-config.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Router-IS-IS Configuration</div></div> <div><div>Command Syntax</div><div>log-adjacency-changes</div><div>no log-adjacency-changes</div><div>default log-adjacency-changes</div></div> <div><div>Examples</div><ul style="list-style-type: none">These commands configure the switch to send a syslog message when a neighbor goes up or down. switch(config)#router isis Osiris switch(config-router-isis)#log-adjacency-changes switch(config-router-isis)#These commands configure not to log the peer changes. switch(config)#router isis Osiris switch(config-router-isis)#no log-adjacency-changes switch(config-router-isis)#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1692.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1452.</div>
	Release	Modification										
4.0(1)	This command was introduced.											
Command	Description											
feature isis	Enables IS-IS on the router.											
router isis	Enables IS-IS.											

Copyright Registration Information	Cisco	Arista										
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>log-adjacency-changes (IS-IS)</div> <p>To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the log-adjacency-changes configuration mode command. To disable this function, use the no form of this command.</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>This command is enabled by default.</div></div> <div><div>Command Modes</div><div>Router configuration VRF configuration</div></div> <div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div> <div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div> <div><div>Usage Guidelines</div><div>The log-adjacency-changes command is on by default but only up/down (full/down) events are reported.</div></div> <div><div>Examples</div><div>This example configures the router to send a syslog message when an IS-IS neighbor state changes: switch(config)# router isis switch(config-router)# log-adjacency-changes</div></div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.	<div>log-adjacency-changes (IS-IS)</div> <p>The log-adjacency-changes command configures the switch to send syslog messages either when it detects IS-IS link state changes or when it detects that a neighbor has gone up or down. Log message sending is disabled by default.</p> <p>The default option is active when running-config does not contain any form of the command. Entering the command in any form replaces the previous command state in running-config.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Router-IS-IS Configuration</div></div> <div><div>Command Syntax</div><div>log-adjacency-changes</div><div>no log-adjacency-changes</div><div>default log-adjacency-changes</div></div> <div><div>Examples</div><ul style="list-style-type: none">These commands configure the switch to send a syslog message when a neighbor goes up or down. switch(config)#router isis Osiris switch(config-router-isis)#log-adjacency-changes switch(config-router-isis)#These commands configure not to log the peer changes. switch(config)#router isis Osiris switch(config-router-isis)#no log-adjacency-changes switch(config-router-isis)#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1692.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1452.</div>
	Release	Modification										
4.0(1)	This command was introduced.											
Command	Description											
feature isis	Enables IS-IS on the router.											
router isis	Enables IS-IS.											

Copyright Registration Information	Cisco	Arista										
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	<div>log-adjacency-changes (IS-IS)</div> <p>To enable the router to send a syslog message when an Intermediate System-to-Intermediate System Intradomain Routing Protocol (IS-IS) neighbor goes up or down, use the log-adjacency-changes configuration mode command. To disable this function, use the no form of this command.</p> <div>log-adjacency-changes</div> <div>no log-adjacency-changes</div> <div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div> <div><div>Defaults</div><div>This command is enabled by default.</div></div> <div><div>Command Modes</div><div>Router configuration VRF configuration</div></div> <div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div> <div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div> <div><div>Usage Guidelines</div><div>The log-adjacency-changes command is on by default but only up/down (full/down) events are reported.</div></div> <div><div>Examples</div><div>This example configures the router to send a syslog message when an IS-IS neighbor state changes: switch(config)# router isis switch(config-router)# log-adjacency-changes</div></div> <div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>feature isis</td><td>Enables IS-IS on the router.</td></tr><tr><td>router isis</td><td>Enables IS-IS.</td></tr></table></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	feature isis	Enables IS-IS on the router.	router isis	Enables IS-IS.	<div>log-adjacency-changes (IS-IS)</div> <p>The log-adjacency-changes command configures the switch to send syslog messages either when it detects IS-IS link state changes or when it detects that a neighbor has gone up or down. Log message sending is disabled by default.</p> <p>The default option is active when running-config does not contain any form of the command. Entering the command in any form replaces the previous command state in running-config.</p> <div><div>Platform</div><div>all</div></div> <div><div>Command Mode</div><div>Router-IS-IS Configuration</div></div> <div><div>Command Syntax</div><div>log-adjacency-changes</div><div>no log-adjacency-changes</div><div>default log-adjacency-changes</div></div> <div><div>Examples</div><ul style="list-style-type: none">These commands configure the switch to send a syslog message when a neighbor goes up or down. switch(config)#router isis Osiris switch(config-router-isis)#log-adjacency-changes switch(config-router-isis)#These commands configure not to log the peer changes. switch(config)#router isis Osiris switch(config-router-isis)#no log-adjacency-changes switch(config-router-isis)#</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1692.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1452.</div>
	Release	Modification										
4.0(1)	This command was introduced.											
Command	Description											
feature isis	Enables IS-IS on the router.											
router isis	Enables IS-IS.											
Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-235.												

Copyright Registration Information	Cisco	Arista																				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div>max-metric router-lsa (OSPF)</div><div><p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the <code>max-metric router-lsa</code> command. To disable the advertisement of a maximum metric, use the <code>no</code> form of this command.</p><pre>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><pre>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><table><tr><td><code>external-lsa</code></td><td>Specifies the external LSA's.</td></tr><tr><td><code>max-metric-value</code></td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td><code>include-stub</code></td><td>Advertises the max-metric for stub links.</td></tr><tr><td><code>on-startup</code></td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td><code>seconds</code></td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td><code>wait-for bgp tag</code></td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td><code>summary-lsa</code></td><td>Specifies the summary LSA's.</td></tr><tr><td><code>max-metric-value</code></td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div></div>	<code>external-lsa</code>	Specifies the external LSA's.	<code>max-metric-value</code>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	<code>include-stub</code>	Advertises the max-metric for stub links.	<code>on-startup</code>	(Optional) Configures the router to advertise a maximum metric at startup.	<code>seconds</code>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	<code>wait-for bgp tag</code>	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	<code>summary-lsa</code>	Specifies the summary LSA's.	<code>max-metric-value</code>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div><div>max-metric router-lsa (OSPFv2)</div><div><p>The <code>max-metric router-lsa</code> command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p><p>The <code>no max-metric router-lsa</code> and <code>default max-metric router-lsa</code> commands disable the advertisement of a maximum metric.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF Configuration</div></div><div><div>Command Syntax</div><pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><p>All parameters can be placed in any order.</p><div><div>Parameters</div><div><ul style="list-style-type: none"><code>EXTERNAL</code> advertised metric value. Values include:<ul style="list-style-type: none"><code><no parameter></code> Metric is set to the default value of 1.<code>external-lsa</code> Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.<code>external-lsa <1 to 16777215></code> The configurable range is from 1 to 0xFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.<code>STUB</code> advertised metric type. Values include:<ul style="list-style-type: none"><code><no parameter></code> Metric type is set to the default value of 2.<code>include-stub</code> Advertises stub links in router-LSA with the max-metric value (0xFFFF).<code>STARTUP</code> limit scope of LSAs. Values include:<ul style="list-style-type: none"><code><no parameter></code> LSA can be translated<code>on-startup</code> Configures the router to advertise a maximum metric at startup (only valid in <code>no</code> and <code>default</code> command formats).<code>on-startup wait-for-bgp</code> Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.<code>on-startup <5 to 86400></code> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.<code>wait-for-bgp</code> or an <code>on-start</code> time value is not included in <code>no</code> and <code>default</code> commands.<code>SUMMARY</code> advertised metric value. Values include:<ul style="list-style-type: none"><code><no parameter></code> Metric is set to the default value of 1.<code>summary-lsa</code> Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.<code>summary-lsa <1 to 16777215></code> Metric is set to the specified value.</div></div></div></div></div>
	<code>external-lsa</code>	Specifies the external LSA's.																				
<code>max-metric-value</code>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																					
<code>include-stub</code>	Advertises the max-metric for stub links.																					
<code>on-startup</code>	(Optional) Configures the router to advertise a maximum metric at startup.																					
<code>seconds</code>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																					
<code>wait-for bgp tag</code>	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																					
<code>summary-lsa</code>	Specifies the summary LSA's.																					
<code>max-metric-value</code>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																					
Release	Modification																					
4.0(1)	This command was introduced.																					

<div>Copyright Registration Information</div>	<div>Cisco</div> <div><div><div>max-metric router-lsa (OSPF)</div><div><p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</p><pre>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><pre>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><table><tr><td>external-lsa</td><td>Specifies the external LSA's.</td></tr><tr><td><i>max-metric-value</i></td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td>include-stub</td><td>Advertises the max-metric for stub links.</td></tr><tr><td>on-startup</td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td><i>seconds</i></td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td>wait-for bgp tag</td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td>summary-lsa</td><td>Specifies the summary LSA's.</td></tr><tr><td><i>max-metric-value</i></td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table></div><div><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div></div><div><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-457</div><div>Cisco NX-OS 5.0</div><div>Effective date of registration: 11/13/2014</div></div></div></div>	external-lsa	Specifies the external LSA's.	<i>max-metric-value</i>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	include-stub	Advertises the max-metric for stub links.	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.	<i>seconds</i>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	summary-lsa	Specifies the summary LSA's.	<i>max-metric-value</i>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div>Arista</div> <div><div><div>max-metric router-lsa (OSPFv2)</div><div><p>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p><p>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</p><p>Platform all Command Mode Router-OSPF Configuration</p><div>Command Syntax<div><pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre></div><p>All parameters can be placed in any order.</p><div>Parameters<ul style="list-style-type: none">EXTERNAL advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.external-lsa Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.external-lsa <1 to 16777215> The configurable range is from 1 to 0xFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.STUB advertised metric type. Values include:<ul style="list-style-type: none"><no parameter> Metric type is set to the default value of 2.include-stub Advertises stub links in router-LSA with the max-metric value (0xFFFF).STARTUP limit scope of LSAs. Values include:<ul style="list-style-type: none"><no parameter> LSA can be translatedon-startup Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).on-startup wait-for-bgp Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.on-startup <5 to 86400> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.wait-for-bgp or an on-start time value is not included in no and default commands.SUMMARY advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.summary-lsa Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.summary-lsa <1 to 16777215> Metric is set to the specified value.</div></div></div></div><div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1439.</div></div></div>
external-lsa	Specifies the external LSA's.																					
<i>max-metric-value</i>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																					
include-stub	Advertises the max-metric for stub links.																					
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.																					
<i>seconds</i>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																					
wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																					
summary-lsa	Specifies the summary LSA's.																					
<i>max-metric-value</i>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																					
Release	Modification																					
4.0(1)	This command was introduced.																					

<div>Copyright Registration Information</div>	<div>Cisco</div> <div><div><div>max-metric router-lsa (OSPF)</div><div><div><div>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</div><div><div><div>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</div><div><div>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</div></div></div><div><div><div><div>external-lsa</div><div>Specifies the external LSA's.</div></div><div><div>max-metric-value</div><div>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</div></div><div><div>include-stub</div><div>Advertises the max-metric for stub links.</div></div><div><div>on-startup</div><div>(Optional) Configures the router to advertise a maximum metric at startup.</div></div><div><div>seconds</div><div>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</div></div><div><div>wait-for bgp tag</div><div>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</div></div><div><div>summary-lsa</div><div>Specifies the summary LSA's.</div></div><div><div>max-metric-value</div><div>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</div></div></div></div><div><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div><div><div><div>Command History</div><div><div><div>Release</div><div>Modification</div></div><div><div>4.0(1)</div><div>This command was introduced.</div></div></div></div></div></div><div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-272</div></div></div></div></div></div></div></div>	<div>Arista</div> <div><div><div>max-metric router-lsa (OSPFv2)</div><div><div><div>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</div><div><div>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</div></div></div><div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF Configuration</div></div></div><div><div><div>Command Syntax</div><div><div><div>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div><div><div>no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div><div><div>default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</div></div></div><div><div>All parameters can be placed in any order.</div></div></div><div><div><div>Parameters</div><div><div><div><div><div>EXTERNAL</div><div>advertised metric value. Values include:</div><div><div><div><no parameter></div><div>Metric is set to the default value of 1.</div></div><div><div>external-lsa</div><div>Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.</div></div><div><div>external-lsa <1 to 16777215></div><div>The configurable range is from 1 to 0xFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.</div></div></div></div><div><div><div>STUB</div><div>advertised metric type. Values include:</div><div><div><div><no parameter></div><div>Metric type is set to the default value of 2.</div></div><div><div>include-stub</div><div>Advertises stub links in router-LSA with the max-metric value (0xFFFF).</div></div></div></div><div><div><div>STARTUP</div><div>limit scope of LSAs. Values include:</div><div><div><div><no parameter></div><div>LSA can be translated</div></div><div><div>on-startup</div><div>Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).</div></div><div><div>on-startup wait-for-bgp</div><div>Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</div></div><div><div>on-startup <5 to 86400></div><div>Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.</div></div><div><div>wait-for-bgp</div><div>or an on-start time value is not included in no and default commands.</div></div></div></div><div><div><div>SUMMARY</div><div>advertised metric value. Values include:</div><div><div><div><no parameter></div><div>Metric is set to the default value of 1.</div></div><div><div>summary-lsa</div><div>Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.</div></div><div><div>summary-lsa <1 to 16777215></div><div>Metric is set to the specified value.</div></div></div></div></div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1439.</div></div></div></div></div></div></div></div></div></div></div>
---	--	--

Cisco NX-OS 4.0

Effective date of registration:
11/13/2014

Copyright Registration Information	Cisco	Arista																				
Cisco IOS 15.0 Effective date of registration: 11/28/2014	<div><div>max-metric router-lsa (OSPF)</div><div><p>To configure the Open Shortest Path First (OSPF) protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their shortest path first (SPF) calculations, use the max-metric router-lsa command. To disable the advertisement of a maximum metric, use the no form of this command.</p><pre>max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><pre>no max-metric router-lsa [external-lsa [max-metric-value]] [include-stub] [on-startup [seconds] wait-for bgp tag] [summary-lsa [max-metric-value]]</pre><table><tr><td>external-lsa</td><td>Specifies the external LSA's.</td></tr><tr><td><i>max-metric-value</i></td><td>(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.</td></tr><tr><td>include-stub</td><td>Advertises the max-metric for stub links.</td></tr><tr><td>on-startup</td><td>(Optional) Configures the router to advertise a maximum metric at startup.</td></tr><tr><td><i>seconds</i></td><td>(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.</td></tr><tr><td>wait-for bgp tag</td><td>(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.</td></tr><tr><td>summary-lsa</td><td>Specifies the summary LSA's.</td></tr><tr><td><i>max-metric-value</i></td><td>(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.</td></tr></table><div><div>Defaults</div><div>Originates router link-state advertisements (LSAs) with normal link metrics.</div></div><div><div>Command Modes</div><div>Router configuration Router VRF configuration</div></div><div><div>Supported User Roles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div></div></div>	external-lsa	Specifies the external LSA's.	<i>max-metric-value</i>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.	include-stub	Advertises the max-metric for stub links.	on-startup	(Optional) Configures the router to advertise a maximum metric at startup.	<i>seconds</i>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.	wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.	summary-lsa	Specifies the summary LSA's.	<i>max-metric-value</i>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.	Release	Modification	4.0(1)	This command was introduced.	<div><div>max-metric router-lsa (OSPFv2)</div><div><p>The max-metric router-lsa command allows the OSPF protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p><p>The no max-metric router-lsa and default max-metric router-lsa commands disable the advertisement of a maximum metric.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Router-OSPF Configuration</div></div><div><div>Command Syntax</div><pre>max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>no max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><pre>default max-metric router-lsa [EXTERNAL] [STUB] [STARTUP] [SUMMARY]</pre><p>All parameters can be placed in any order.</p><div><div>Parameters</div><div><ul style="list-style-type: none">EXTERNAL advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.external-lsa Configures the router to override the External LSA / NSSA-External metric with the maximum metric value.external-lsa <1 to 16777215> The configurable range is from 1 to 0xFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA.STUB advertised metric type. Values include:<ul style="list-style-type: none"><no parameter> Metric type is set to the default value of 2.include-stub Advertises stub links in router-LSA with the max-metric value (0xFFFF).STARTUP limit scope of LSAs. Values include:<ul style="list-style-type: none"><no parameter> LSA can be translatedon-startup Configures the router to advertise a maximum metric at startup (only valid in no and default command formats).on-startup wait-for-bgp Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.on-startup <5 to 86400> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value.wait-for-bgp or an on-start time value is not included in no and default commands.SUMMARY advertised metric value. Values include:<ul style="list-style-type: none"><no parameter> Metric is set to the default value of 1.summary-lsa Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs.summary-lsa <1 to 16777215> Metric is set to the specified value.</div></div></div></div></div>
	external-lsa	Specifies the external LSA's.																				
<i>max-metric-value</i>	(Optional) Specifies the max-metric values for external LSA's. The range is 1-65535.																					
include-stub	Advertises the max-metric for stub links.																					
on-startup	(Optional) Configures the router to advertise a maximum metric at startup.																					
<i>seconds</i>	(Optional) Maximum metric (in seconds) that is advertised for the specified time interval. The configurable range is from 5 to 86400 seconds. The default is 600 seconds.																					
wait-for bgp tag	(Optional) Advertises a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds.																					
summary-lsa	Specifies the summary LSA's.																					
<i>max-metric-value</i>	(Optional) Specifies the max-metric value for summary LSAs. The range is from 1-65535.																					
Release	Modification																					
4.0(1)	This command was introduced.																					

Copyright Registration Information	Cisco	Arista																																																												
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>BGP table version is 10, local router ID is 3.3.3.3 Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist Origin codes: i - IGP, e - EGP, ? - incomplete - multipath</div> <table><thead><tr><th>Network</th><th>Next Hop</th><th>Metric</th><th>LocPrf</th><th>Weight</th><th>Path</th></tr></thead><tbody><tr><td>* i200.0.1.100/32</td><td>201.0.25.1</td><td></td><td>100</td><td>100</td><td>6553601 i</td></tr><tr><td>*>e</td><td>201.0.13.1</td><td></td><td></td><td>0</td><td>6553601 i</td></tr><tr><td>* i200.0.2.100/32</td><td>201.0.25.1</td><td></td><td>100</td><td>100</td><td>6553601 i</td></tr><tr><td>*>e</td><td>201.0.13.1</td><td></td><td></td><td>0</td><td>6553601 i</td></tr><tr><td>*>i200.0.3.100/32</td><td>0.0.0.0</td><td></td><td>100</td><td>32768</td><td>i</td></tr></tbody></table> <div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 401.</div>	Network	Next Hop	Metric	LocPrf	Weight	Path	* i200.0.1.100/32	201.0.25.1		100	100	6553601 i	*>e	201.0.13.1			0	6553601 i	* i200.0.2.100/32	201.0.25.1		100	100	6553601 i	*>e	201.0.13.1			0	6553601 i	*>i200.0.3.100/32	0.0.0.0		100	32768	i	<div>switch>show ip bgp neighbors 10.14.4.4 advertised-routes regexp _64502_ BGP routing table information for VRF default Router identifier 172.24.78.191, local AS number 64498 Route status codes: s - suppressed, * - valid, > - active, E - ECMP head, e - ECMP S - Stale Origin codes: i - IGP, e - EGP, ? - incomplete AS Path Attributes: Or-ID - Originator ID, C-LST - Cluster List, LL Nexthop - Link Local Nexthop</div> <table><thead><tr><th>Network</th><th>Next Hop</th><th>Metric</th><th>LocPrf</th><th>Weight</th><th>Path</th></tr></thead><tbody><tr><td>* > 10.99.31.0/24</td><td>10.88.202.1</td><td>333</td><td>100</td><td>-</td><td>(64502 64503) 99 i</td></tr><tr><td>* > 10.99.41.0/24</td><td>10.88.202.1</td><td>333</td><td>100</td><td>-</td><td>(64502 64503) 99 i</td></tr><tr><td>* > 10.99.99.0/24</td><td>10.88.202.1</td><td>333</td><td>100</td><td>-</td><td>(64502 64504) 99 i</td></tr></tbody></table> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1637.</div>	Network	Next Hop	Metric	LocPrf	Weight	Path	* > 10.99.31.0/24	10.88.202.1	333	100	-	(64502 64503) 99 i	* > 10.99.41.0/24	10.88.202.1	333	100	-	(64502 64503) 99 i	* > 10.99.99.0/24	10.88.202.1	333	100	-	(64502 64504) 99 i
Network	Next Hop	Metric	LocPrf	Weight	Path																																																									
* i200.0.1.100/32	201.0.25.1		100	100	6553601 i																																																									
*>e	201.0.13.1			0	6553601 i																																																									
* i200.0.2.100/32	201.0.25.1		100	100	6553601 i																																																									
*>e	201.0.13.1			0	6553601 i																																																									
*>i200.0.3.100/32	0.0.0.0		100	32768	i																																																									
Network	Next Hop	Metric	LocPrf	Weight	Path																																																									
* > 10.99.31.0/24	10.88.202.1	333	100	-	(64502 64503) 99 i																																																									
* > 10.99.41.0/24	10.88.202.1	333	100	-	(64502 64503) 99 i																																																									
* > 10.99.99.0/24	10.88.202.1	333	100	-	(64502 64504) 99 i																																																									
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>show ip bgp neighbors</div> <div>To display Border Gateway Protocol (BGP) neighbors, use the show ip bgp neighbors command.</div> <div>show ip bgp neighbors [addr] advertised-routes flap-statistics paths received-routes routes [advertised dampened received] prefix vrf { all vrf-name }</div> <table><thead><tr><th>Syntax</th><th>Description</th></tr></thead><tbody><tr><td>addr</td><td>IPv4 address. The format is x.x.x.x</td></tr><tr><td>advertised-routes</td><td>(Optional) Displays all the routes advertised to this neighbor.</td></tr><tr><td>flap-statistics</td><td>(Optional) Displays flap statistics for the routes received from this neighbor.</td></tr><tr><td>paths</td><td>(Optional) Displays AS paths learned from this neighbor.</td></tr><tr><td>received-routes</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td>routes</td><td>(Optional) Displays the routes received or advertised to or from this neighbor.</td></tr><tr><td>advertised</td><td>(Optional) Displays all the routes advertised for this neighbor.</td></tr><tr><td>dampened</td><td>(Optional) Displays all dampened routes received from this neighbor.</td></tr><tr><td>received</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td>prefix</td><td>(Optional) IPv6 prefix. The format is x.x.x.x/length.</td></tr><tr><td>vrf vrf-name</td><td>(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.</td></tr><tr><td>all</td><td>(Optional) Specifies all VRF.</td></tr></tbody></table> <div>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 466.</div>	Syntax	Description	addr	IPv4 address. The format is x.x.x.x	advertised-routes	(Optional) Displays all the routes advertised to this neighbor.	flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.	paths	(Optional) Displays AS paths learned from this neighbor.	received-routes	(Optional) Displays all the routes received from this neighbor.	routes	(Optional) Displays the routes received or advertised to or from this neighbor.	advertised	(Optional) Displays all the routes advertised for this neighbor.	dampened	(Optional) Displays all dampened routes received from this neighbor.	received	(Optional) Displays all the routes received from this neighbor.	prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length.	vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.	all	(Optional) Specifies all VRF.	<div>show ip bgp neighbors</div> <div>The show ip bgp neighbors command displays Border Gateway Protocol (BGP) and TCP session data for a specified IPv4 BGP neighbor, or for all IPv4 BGP neighbors if an address is not included.</div> <div>Platform all Command Mode EXEC</div> <div>Command Syntax</div> <div>show ip bgp neighbors [NEIGHBOR_ADDR] [VRF_INSTANCE]</div> <div>Parameters</div> <div><ul style="list-style-type: none">NEIGHBOR_ADDR location of neighbors. Options include:<ul style="list-style-type: none"><no parameter> command displays information for all IPv4 BGP neighbors.ipv4 addr command displays information for specified neighbor.VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRF.vrf vrf name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF.</div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1632.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1402; Arista User Manual, v. 4.11.1 (1/11/13), at 1148; Arista User Manual v. 4.10.3 (10/22/12), at 959.</div>																																		
Syntax	Description																																																													
addr	IPv4 address. The format is x.x.x.x																																																													
advertised-routes	(Optional) Displays all the routes advertised to this neighbor.																																																													
flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.																																																													
paths	(Optional) Displays AS paths learned from this neighbor.																																																													
received-routes	(Optional) Displays all the routes received from this neighbor.																																																													
routes	(Optional) Displays the routes received or advertised to or from this neighbor.																																																													
advertised	(Optional) Displays all the routes advertised for this neighbor.																																																													
dampened	(Optional) Displays all dampened routes received from this neighbor.																																																													
received	(Optional) Displays all the routes received from this neighbor.																																																													
prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length.																																																													
vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.																																																													
all	(Optional) Specifies all VRF.																																																													

Copyright Registration Information	Cisco	Arista																																				
	<div>show ip bgp neighbors</div> <p>To display Border Gateway Protocol (BGP) neighbors, use the <code>show ip bgp neighbors</code> command.</p> <div>show ip bgp neighbors [addr] [advertised-routes flap-statistics paths received-routes routes [advertised dampened received]] [prefix] [vrf { all vrf-name }]</div> <table><tr><td>Syntax Description</td><td>addr</td><td>IPv4 address. The format is x.x.x.x.</td></tr><tr><td></td><td>advertised-routes</td><td>(Optional) Displays all the routes advertised to this neighbor.</td></tr><tr><td></td><td>flap-statistics</td><td>(Optional) Displays flap statistics for the routes received from this neighbor.</td></tr><tr><td></td><td>paths</td><td>(Optional) Displays AS paths learned from this neighbor.</td></tr><tr><td></td><td>received-routes</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td></td><td>routes</td><td>(Optional) Displays the routes received or advertised to or from this neighbor.</td></tr><tr><td></td><td>advertised</td><td>(Optional) Displays all the routes advertised for this neighbor.</td></tr><tr><td></td><td>dampened</td><td>(Optional) Displays all dampened routes received from this neighbor.</td></tr><tr><td></td><td>received</td><td>(Optional) Displays all the routes received from this neighbor.</td></tr><tr><td></td><td>prefix</td><td>(Optional) IPv6 prefix. The format is x.x.x.x/length.</td></tr><tr><td></td><td>vrf vrf-name</td><td>(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.</td></tr><tr><td></td><td>all</td><td>(Optional) Specifies all VRF.</td></tr></table>	Syntax Description	addr	IPv4 address. The format is x.x.x.x.		advertised-routes	(Optional) Displays all the routes advertised to this neighbor.		flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.		paths	(Optional) Displays AS paths learned from this neighbor.		received-routes	(Optional) Displays all the routes received from this neighbor.		routes	(Optional) Displays the routes received or advertised to or from this neighbor.		advertised	(Optional) Displays all the routes advertised for this neighbor.		dampened	(Optional) Displays all dampened routes received from this neighbor.		received	(Optional) Displays all the routes received from this neighbor.		prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length.		vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.		all	(Optional) Specifies all VRF.	<div>show ip bgp neighbors</div> <p>The <code>show ip bgp neighbors</code> command displays Border Gateway Protocol (BGP) and TCP session data for a specified IPv4 BGP neighbor, or for all IPv4 BGP neighbors if an address is not included.</p> <p>Platform all Command Mode EXEC</p> <p>Command Syntax</p> <div>show ip bgp neighbors [NEIGHBOR_ADDR] [VRF_INSTANCE]</div> <p>Parameters</p> <ul style="list-style-type: none">NEIGHBOR_ADDR location of neighbors. Options include:<ul style="list-style-type: none"><no parameter> command displays information for all IPv4 BGP neighbors.ipv4 addr command displays information for specified neighbor.VRF_INSTANCE specifies VRF instances.<ul style="list-style-type: none"><no parameter> displays routing table for context-active VRF.vrf vrf_name displays routing table for the specified VRF.vrf all displays routing table for all VRFs.vrf default displays routing table for default VRF.
Syntax Description	addr	IPv4 address. The format is x.x.x.x.																																				
	advertised-routes	(Optional) Displays all the routes advertised to this neighbor.																																				
	flap-statistics	(Optional) Displays flap statistics for the routes received from this neighbor.																																				
	paths	(Optional) Displays AS paths learned from this neighbor.																																				
	received-routes	(Optional) Displays all the routes received from this neighbor.																																				
	routes	(Optional) Displays the routes received or advertised to or from this neighbor.																																				
	advertised	(Optional) Displays all the routes advertised for this neighbor.																																				
	dampened	(Optional) Displays all dampened routes received from this neighbor.																																				
	received	(Optional) Displays all the routes received from this neighbor.																																				
	prefix	(Optional) IPv6 prefix. The format is x.x.x.x/length.																																				
	vrf vrf-name	(Optional) Specifies the virtual router context (VRF) name. The name can be any case-sensitive, alphanumeric string up to 63 characters.																																				
	all	(Optional) Specifies all VRF.																																				
Cisco NX-OS 5.0	Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-686.	Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1632.																																				
Effective date of registration: 11/13/2014		See also Arista User Manual v. 4.12.3 (7/17/13), at 1402; Arista User Manual, v. 4.11.1 (1/11/13), at 1148; Arista User Manual v. 4.10.3 (10/22/12), at 959.																																				

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Use the <code>ip ospf database</code> command to display information about different OSPF LSAs.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network's IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements). • A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) • When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. • When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 520.</p>	<ul style="list-style-type: none"> • <i>linkstate_id</i> Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. <ul style="list-style-type: none"> — When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following: <ul style="list-style-type: none"> The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Use the <code>ip ospf database</code> command to display information about different OSPF LSAs.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network's IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements). • A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) • When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. • When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 5.x (2010), at L3-742.</p>	<ul style="list-style-type: none"> • <i>linkstate_id</i> Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. <ul style="list-style-type: none"> — When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following: <ul style="list-style-type: none"> The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Use the <code>ip ospf database</code> command to display information about different OSPF LSAs.</p> <p>When the link state advertisement is describing a network, the <i>link-state-id</i> argument can take one of two forms:</p> <ul style="list-style-type: none"> • The network's IP address (such as Type 3 summary link advertisements and autonomous system external link advertisements). • A derived address obtained from the link state ID. (Note that masking a network links advertisement's link state ID with the network's subnet mask yields the network's IP address.) • When the link state advertisement is describing a router, the link state ID is always the described router's OSPF router ID. • When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0). <p>This command requires the Enterprise Services license.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference, Release 4.x (2008), at L3-426.</p>	<ul style="list-style-type: none"> • <i>linkstate_id</i> Network segment described by the LSA (dotted decimal notation). Value depends on the LSA type. <ul style="list-style-type: none"> — When the LSA describes a network, the <i>linkstate-id</i> argument is one of the following: <ul style="list-style-type: none"> The network IP address, as in Type 3 summary link advertisements and in autonomous system external link advertisements. A derived address obtained from the link state ID. Masking a network links the advertisement link state ID with the network subnet mask yielding the network IP address. — When the LSA describes a router, the link state ID is the OSPFv2 router ID of the router. — When an autonomous system external advertisement (Type 5) describes a default route, its link state ID is set to the default destination (0.0.0.0). <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1454.</p> <p><i>See also</i> Arista User Manual v. 4.13.6F (4/14/2014), at 1404; Arista User Manual v. 4.12.3 (7/17/13), at 1240; Arista User Manual, v. 4.11.1 (1/11/13), at 996; Arista User Manual v. 4.10.3 (10/22/12), at 825; Arista User Manual v. 4.9.3.2 (5/3/12), at 648; Arista User Manual v. 4.8.2 at 483; Arista User Manual v. 4.7.3 (7/18/11), at 357; Arista User Manual v. 4.6.0 (12/22/2010), at 217</p>

Copyright Registration Information	Cisco	Arista																								
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>timers lsa-arrival (OSPF)</div><div><div>To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the timers lsa-arrival command. To return to the default, use the no form of this command.</div><div><div>timers lsa-arrival milliseconds</div><div>no timers lsa-arrival</div></div></div><table><tr><td>Syntax Description</td><td>milliseconds</td><td>Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr><tr><td>Defaults</td><td colspan="2">1000 milliseconds</td></tr><tr><td>Command Modes</td><td colspan="2">Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2"><div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div><div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div><div>This command requires the Enterprise Services license.</div></td></tr><tr><td></td><td>Examples</td><td><div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div><div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div></td></tr></table></div>	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.	Defaults	1000 milliseconds		Command Modes	Router configuration VRF configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>			Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>	<div><div>timers lsa arrival (OSPFv2)</div><div><div>The timers lsa arrival command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</div><div>The no timers lsa arrival and default timers lsa arrival commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the timers lsa arrival command from running-config.</div><div><div>Platformall</div><div>Command ModeRouter-OSPF Configuration</div></div><div><div>Command Syntax</div><div>timers lsa arrival lsa_time no timers lsa arrival default timers lsa arrival</div></div><div><div>Parameters</div><div><div>lsa_time</div><div>OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.</div></div></div><div><div>Example</div><div><div>This command sets the minimum interval timer to ten milliseconds.</div><div>switch(config)#router ospf 6 switch(config-router-ospf)#timers lsa arrival 10 switch(config-router-ospf)#</div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1469.</div></div>
	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.																							
Defaults	1000 milliseconds																									
Command Modes	Router configuration VRF configuration																									
Supported User Roles	network-admin vdc-admin																									
Command History	Release	Modification																								
	4.0(1)	This command was introduced.																								
Usage Guidelines	<div>Use the timers lsa arrival command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</div> <div>We recommend that you keep the milliseconds value of the timers lsa-arrival command less than or equal to the neighbors' hold-interval value of the timers throttle lsa command.</div> <div>This command requires the Enterprise Services license.</div>																									
	Examples	<div>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</div> <div>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</div>																								

Copyright Registration Information	Cisco	Arista																								
<div>Cisco NX-OS 4.0</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>timers lsa-arrival (OSPF)</div><div><p>To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the <code>timers lsa-arrival</code> command. To return to the default, use the <code>no</code> form of this command.</p><div><div>timers lsa-arrival milliseconds</div><div>no timers lsa-arrival</div></div></div><table><tr><td>Syntax Description</td><td>milliseconds</td><td>Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr><tr><td>Defaults</td><td colspan="2">1000 milliseconds</td></tr><tr><td>Command Modes</td><td colspan="2">Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>4.0(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2"><p>Use the <code>timers lsa arrival</code> command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</p><p>We recommend that you keep the <i>milliseconds</i> value of the <code>timers lsa-arrival</code> command less than or equal to the neighbors' <i>hold-interval</i> value of the <code>timers throttle lsa</code> command.</p><p>This command requires the Enterprise Services license.</p></td></tr><tr><td>Examples</td><td colspan="2"><p>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</p><div><div>switch(config)# router ospf 1</div><div>switch(config-router)# timers lsa-arrival 2000</div></div></td></tr></table></div>	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.	Defaults	1000 milliseconds		Command Modes	Router configuration VRF configuration		Supported User Roles	network-admin vdc-admin		Command History	Release	Modification		4.0(1)	This command was introduced.	Usage Guidelines	<p>Use the <code>timers lsa arrival</code> command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</p> <p>We recommend that you keep the <i>milliseconds</i> value of the <code>timers lsa-arrival</code> command less than or equal to the neighbors' <i>hold-interval</i> value of the <code>timers throttle lsa</code> command.</p> <p>This command requires the Enterprise Services license.</p>		Examples	<p>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</p> <div><div>switch(config)# router ospf 1</div><div>switch(config-router)# timers lsa-arrival 2000</div></div>		<div><div>timers lsa arrival (OSPFv2)</div><div><p>The <code>timers lsa arrival</code> command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</p><p>The <code>no timers lsa arrival</code> and default <code>timers lsa arrival</code> commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the <code>timers lsa arrival</code> command from <i>running-config</i>.</p><div><div>Platformall</div><div>Command ModeRouter-OSPF Configuration</div></div><div><div>Command Syntax</div><div><div>timers lsa arrival lsa_time</div><div>no timers lsa arrival</div><div>default timers lsa arrival</div></div></div><div><div>Parameters</div><div><ul style="list-style-type: none"><i>lsa_time</i> OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.</div></div><div><div>Example</div><div><ul style="list-style-type: none">This command sets the minimum interval timer to ten milliseconds.<div><div>switch(config)#router ospf 6</div><div>switch(config-router-ospf)#timers lsa arrival 10</div><div>switch(config-router-ospf)#</div></div></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1469.</div></div>
	Syntax Description	milliseconds	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.																							
Defaults	1000 milliseconds																									
Command Modes	Router configuration VRF configuration																									
Supported User Roles	network-admin vdc-admin																									
Command History	Release	Modification																								
	4.0(1)	This command was introduced.																								
Usage Guidelines	<p>Use the <code>timers lsa arrival</code> command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</p> <p>We recommend that you keep the <i>milliseconds</i> value of the <code>timers lsa-arrival</code> command less than or equal to the neighbors' <i>hold-interval</i> value of the <code>timers throttle lsa</code> command.</p> <p>This command requires the Enterprise Services license.</p>																									
Examples	<p>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</p> <div><div>switch(config)# router ospf 1</div><div>switch(config-router)# timers lsa-arrival 2000</div></div>																									

Copyright Registration Information	Cisco	Arista																									
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	<div>timers lsa-arrival (OSPF)</div> <div><p>To set the minimum interval in which the software accepts the same link-state advertisement (LSA) from Open Shortest Path First (OSPF) neighbors, use the <code>timers lsa-arrival</code> command. To return to the default, use the <code>no</code> form of this command.</p><div><code>timers lsa-arrival</code> <i>milliseconds</i></div><div><code>no timers lsa-arrival</code></div></div> <table><tr><td>Syntax Description</td><td><i>milliseconds</i></td><td>Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.</td></tr><tr><td>Defaults</td><td colspan="2">1000 milliseconds</td></tr><tr><td>Command Modes</td><td colspan="2">Router configuration VRF configuration</td></tr><tr><td>Supported User Roles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></td><td></td></tr><tr><td>Usage Guidelines</td><td colspan="2"><p>Use the <code>timers lsa arrival</code> command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</p><p>We recommend that you keep the <i>milliseconds</i> value of the <code>timers lsa-arrival</code> command less than or equal to the neighbors' <i>hold-interval</i> value of the <code>timers throttle lsa</code> command.</p><p>This command requires the Enterprise Services license.</p></td></tr><tr><td>Examples</td><td colspan="2"><p>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</p><pre>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</pre></td></tr></table>	Syntax Description	<i>milliseconds</i>	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.	Defaults	1000 milliseconds		Command Modes	Router configuration VRF configuration		Supported User Roles	network-admin vdc-admin		Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.		Usage Guidelines	<p>Use the <code>timers lsa arrival</code> command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</p> <p>We recommend that you keep the <i>milliseconds</i> value of the <code>timers lsa-arrival</code> command less than or equal to the neighbors' <i>hold-interval</i> value of the <code>timers throttle lsa</code> command.</p> <p>This command requires the Enterprise Services license.</p>		Examples	<p>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</p> <pre>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</pre>		<div>timers lsa arrival (OSPFv2)</div> <div><p>The <code>timers lsa arrival</code> command sets the minimum interval in which the switch accepts the same link-state advertisement (LSA) from OSPF neighbors.</p><p>The <code>no timers lsa arrival</code> and default <code>timers lsa arrival</code> commands restore the default maximum OSPFv2 path calculation interval to five seconds by removing the <code>timers lsa arrival</code> command from <i>running-config</i>.</p><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Router-OSPF Configuration</div></div><div>Command Syntax</div><div><code>timers lsa arrival</code> <i>lsa_time</i> <code>no timers lsa arrival</code> <code>default timers lsa arrival</code></div><div>Parameters</div><div><ul style="list-style-type: none"><i>lsa_time</i> OSPFv2 minimum interval (seconds). Values range from 1 to 600000 milliseconds. Default is 1000 milliseconds.</div><div>Example</div><div><ul style="list-style-type: none">This command sets the minimum interval timer to ten milliseconds.<pre>switch(config)#router ospf 6 switch(config-router-ospf)#timers lsa arrival 10 switch(config-router-ospf)#</pre></div></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1469.</div>
	Syntax Description	<i>milliseconds</i>	Minimum delay (in milliseconds) that must pass between acceptance of the same LSA arriving from neighbors. The range is from 10 to 600,000 milliseconds. The default is 1000 milliseconds.																								
Defaults	1000 milliseconds																										
Command Modes	Router configuration VRF configuration																										
Supported User Roles	network-admin vdc-admin																										
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.																						
Release	Modification																										
4.0(1)	This command was introduced.																										
Usage Guidelines	<p>Use the <code>timers lsa arrival</code> command to configure the minimum interval for accepting the same LSA. The same LSA is an LSA instance that contains the same LSA ID number, LSA type, and advertising router ID. If an instance of the same LSA arrives sooner than the interval that is set, the software drops the LSA.</p> <p>We recommend that you keep the <i>milliseconds</i> value of the <code>timers lsa-arrival</code> command less than or equal to the neighbors' <i>hold-interval</i> value of the <code>timers throttle lsa</code> command.</p> <p>This command requires the Enterprise Services license.</p>																										
Examples	<p>This example shows how to set the minimum interval for accepting the same LSA at 2000 milliseconds:</p> <pre>switch(config)# router ospf 1 switch(config-router)# timers lsa-arrival 2000</pre>																										

Copyright Registration Information	Cisco	Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Examples</p> <p>This example shows how to configure a router configured with the start, hold, and maximum interval values for the <code>timers throttle spf</code> command set at 5, 1000, and 90,000 milliseconds:</p> <pre>switch(config)# router ospf 1 switch(config-router)# timers throttle spf 5 1000 90000</pre> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 1033-34.</p>	<p>Example</p> <ul style="list-style-type: none"> This command displays a switch configured with the start, hold, and maximum interval values for the <code>timers throttle spf</code> command set at 5, 1,000, and 20,000 milliseconds, respectively. <pre>switch(config)#router ospf 6 switch(config-router-ospf)#timers spf 5 100 20000 switch(config-router-ospf)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1472.</p>
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference (2013), at 730.</p>	<p><code>cluster-id {cluster-id cluster-ip-addr}</code>—Configures the Route Reflector Cluster-ID (router, vrf). Range: 1 to 4294967295. You can enter the cluster identification as a 32-bit quantity or as an IP address. To remove the cluster ID, use the <code>no</code> form of this command. Together, a route reflector and its clients form a cluster. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.</p> <p>The <code>cluster-id</code> command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1549.</p>
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>The <code>no ip local-proxy-arp</code> and default <code>ip local-proxy-arp</code> commands disable local proxy ARP on the configuration mode interface by removing the corresponding <code>ip local-proxy-arp</code> command from <code>running-config</code>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1276.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 876; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>The <code>no ip local-proxy-arp</code> and default <code>ip local-proxy-arp</code> commands disable local proxy ARP on the configuration mode interface by removing the corresponding <code>ip local-proxy-arp</code> command from <i>running-config</i>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1276.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 876; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Local Proxy ARP</p> <p>You can use local Proxy ARP to enable a device to respond to ARP requests for IP addresses within a subnet where normally no routing is required. When you enable local Proxy ARP, ARP responds to all ARP requests for IP addresses within the subnet and forwards all traffic between hosts in the subnet. Use this feature only on subnets where hosts are intentionally prevented from communicating directly by the configuration on the device to which they are connected.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 2-5.</p>	<p>ip local-proxy-arp</p> <p>The <code>ip local-proxy-arp</code> command enables local proxy ARP (Address Resolution Protocol) on the configuration mode interface. Local proxy ARP programs the switch to respond to ARP requests for IP addresses within a subnet where routing is not normally required. A typical local proxy arp application is supporting isolated private VLANs that communicate with each other by routing packets.</p> <p>The <code>no ip local-proxy-arp</code> and default <code>ip local-proxy-arp</code> commands disable local proxy ARP on the configuration mode interface by removing the corresponding <code>ip local-proxy-arp</code> command from <i>running-config</i>.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1276.</p> <p>See also Arista User Manual v. 4.13.6F (4/14/2014), at 1231; Arista User Manual v. 4.12.3 (7/17/13), at 1073; Arista User Manual, v. 4.11.1 (1/11/13), at 876; Arista User Manual v. 4.10.3 (10/22/12), at 707.</p>

Copyright Registration Information	Cisco		Arista
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.	Router Advertisement Flag Configuration The <code>ipv6 nd managed-config-flag</code> command configures the switch to set the <i>managed address configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This bit instructs receptive hosts to use stateful address autoconfiguration. The <code>ipv6 nd other-config-flag</code> command configures the switch to set the <i>other stateful configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This flag indicates the availability of autoconfiguration information, other than addresses, and that hosts should use stateful
	ipv6 nd mtu	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.	
	ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface.	
	ipv6 nd other-config-flag	Configures the other stateful configuration flag in IPv6 router advertisements.	
	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 3-24.		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1329. See also Arista User Manual v. 4.12.3 (7/17/13), at 1119; Arista User Manual, v. 4.11.1 (1/11/13), at 887; Arista User Manual v. 4.10.3 (10/22/12), at 733.
Cisco NX-OS 5.x Effective date of registration: 11/13/2014	ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.	Router Advertisement Flag Configuration The <code>ipv6 nd managed-config-flag</code> command configures the switch to set the <i>managed address configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This bit instructs receptive hosts to use stateful address autoconfiguration. The <code>ipv6 nd other-config-flag</code> command configures the switch to set the <i>other stateful configuration flag</i> in IPv6 router advertisements transmitted from the configuration mode interface. This flag indicates the availability of autoconfiguration information, other than addresses, and that hosts should use stateful
	ipv6 nd mtu	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.	
	ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface.	
	ipv6 nd other-config-flag	Configures the other stateful configuration flag in IPv6 router advertisements.	
	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 3-22.		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1329. See also Arista User Manual v. 4.12.3 (7/17/13), at 1119; Arista User Manual, v. 4.11.1 (1/11/13), at 887; Arista User Manual v. 4.10.3 (10/22/12), at 733.

Copyright Registration Information	Cisco		Arista
Cisco NX-OS 4.0 Effective date of registration: 11/13/2014	ipv6 nd managed-config-flag	Sets the managed address configuration flag in IPv6 router advertisements.	Router Advertisement Flag Configuration The <code>ipv6 nd managed-config-flag</code> command configures the switch to set the <i>managed address configuration</i> flag in IPv6 router advertisements transmitted from the configuration mode interface. This bit instructs receptive hosts to use stateful address autoconfiguration. The <code>ipv6 nd other-config-flag</code> command configures the switch to set the <i>other stateful configuration</i> flag in IPv6 router advertisements transmitted from the configuration mode interface. This flag indicates the availability of autoconfiguration information, other than addresses, and that hosts should use stateful
	ipv6 nd mtu	Sets the maximum transmission unit (MTU) size of IPv6 packets sent on an interface.	
	ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation retransmissions on an interface.	
	ipv6 nd other-config-flag	Configures the other stateful configuration flag in IPv6 router advertisements.	
Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 3-22.		Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1329. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1119; Arista User Manual, v. 4.11.1 (1/11/13), at 887; Arista User Manual v. 4.10.3 (10/22/12), at 733.	
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	ipv6 nd reachable-time	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.	ipv6 nd reachable-time The <code>ipv6 nd reachable-time</code> command specifies the time period that the switch includes in the reachable time field of Router Advertisements (RAs) sent from the configuration mode interface. The reachable time defines the period that a remote IPv6 node is considered reachable after a reachability confirmation event. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1359. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1149.
	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 3-24.		
Cisco NX-OS 5.0 Effective date of registration: 11/13/2014	ipv6 nd reachable-time	Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.	ipv6 nd reachable-time The <code>ipv6 nd reachable-time</code> command specifies the time period that the switch includes in the reachable time field of Router Advertisements (RAs) sent from the configuration mode interface. The reachable time defines the period that a remote IPv6 node is considered reachable after a reachability confirmation event. Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1359. <i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1149.
	Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 3-22.		



Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="300 277 1142 358"> <div>ipv6 nd reachable-time</div> <div>Configures the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred.</div> </div> <hr/> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 3-22.</p>	<p>ipv6 nd reachable-time</p> <p>The <code>ipv6 nd reachable-time</code> command specifies the time period that the switch includes in the reachable time field of Router Advertisements (RAs) sent from the configuration mode interface. The reachable time defines the period that a remote IPv6 node is considered reachable after a reachability confirmation event.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1359.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1149.</p>


Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Step 3 <code>max-metric router-lsa {external-lsa [max-metric-value]] [stub-prefix-lsa [on-startup [seconds] wait-for-bgp tag]] [inter-area-prefix-lsa [max-metric-sumlsa]]</code></p> <p>Example: <code>switch(config-router)# max-metric router-lsa on-startup wait-for-bgp</code></p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 7-42.</p>	<p>max-metric router-lsa (OSPFv3)</p> <p>The <code>max-metric router-lsa</code> command allows the OSPFv3 protocol to advertise a maximum metric so that other routers do not prefer the router as an intermediate hop in their SPF calculations.</p> <p>The no <code>max-metric router-lsa</code> and default <code>max-metric router-lsa</code> commands disable the advertisement of a maximum metric.</p> <p>Platform all Command Mode Router-OSPF3 Configuration</p> <p>Command Syntax</p> <pre>max-metric router-lsa {EXTERNAL} [STUB] [STARTUP] [SUMMARY] no max-metric router-lsa {EXTERNAL} [STUB] [STARTUP] [SUMMARY] default max-metric router-lsa {EXTERNAL} [STUB] [STARTUP] [SUMMARY]</pre> <p>All parameters can be placed in any order.</p> <p>Parameters</p> <ul style="list-style-type: none"> EXTERNAL advertised metric value. Values include: <ul style="list-style-type: none"> <no parameter> Metric is set to the default value of 1. <code>external-lsa</code> Configures the router to override the External LSA / NSSA-External metric with the maximum metric value. <code>external-lsa <1 to 16777215></code> The configurable range is from 1 to 0xFFFFFFFF. The default value is 0xFF0000. This range can be used with external LSA, summary LSA extensions to indicate the respective metric you want with the LSA. STUB advertised metric type. Values include: <ul style="list-style-type: none"> <no parameter> Metric type is set to the default value of 2. <code>include-stub</code> Advertises stub links in router-LSA with the max-metric value (0xFFFF). STARTUP limit scope of LSAs. Values include: <ul style="list-style-type: none"> <no parameter> LSA can be translated <code>on-startup</code> Configures the router to advertise a maximum metric at startup (only valid in no and default command formats). <code>on-startup wait-for-bgp</code> Configures the router to advertise a maximum metric until Border Gateway Protocol (BGP) routing tables have converged or the default timer has expired. The default timer is 600 seconds. <code>on-startup <5 to 86400></code> Sets the maximum metric temporarily after a reboot to originate router-LSAs with the max-metric value. <p><code>wait-for-bgp</code> or an <code>on-start</code> time value is not included in no and default commands.</p> SUMMARY advertised metric value. Values include: <ul style="list-style-type: none"> <no parameter> Metric is set to the default value of 1. <code>summary-lsa</code> Configures the router to override the summary LSA metric with the maximum metric value for both type 3 and type 4 Summary LSAs. <code>summary-lsa <1 to 16777215></code> Metric is set to the specified value. <p>Example</p> <ul style="list-style-type: none"> This command shows how to configure OSPFv3 to originate router LSAs with the maximum metric until BGP indicates that it has converged: <pre>switch(config-router-ospf3)#max-metric router-lsa on-startup wait-for-bgp switch(config-router-ospf3)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1519.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the “Configuring the Transient Mode for Hello Padding” section on page 9-21.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the “Verifying the IS-IS Configuration” section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-2.</p>	<p>IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. Hello packets – Hello packets, can establish and maintain neighbor relationships. Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the “Configuring the Transient Mode for Hello Padding” section on page 9-21.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the “Verifying the IS-IS Configuration” section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-2.</p>	<p>IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. • IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. • IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. • LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. • Hello packets – Hello packets, can establish and maintain neighbor relationships. • Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>IS-IS Overview</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, such as the authentication, area, and supported protocols, which the receiving interface uses to determine compatibility with the originating interface. The hello packets are also padded to ensure that IS-IS establishes adjacencies only with interfaces that have matching maximum transmission unit (MTU) settings. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). By default, the router sends a periodic LSP refresh every 10 minutes and the LSPs remain in the link-state database for 20 minutes (the LSP lifetime). If the router does not receive an LSP refresh before the end of the LSP lifetime, the router deletes the LSP from the database.</p> <p>The LSP interval must be less than the LSP lifetime or the LSPs time out before they are refreshed.</p> <p>IS-IS sends periodic hello packets to adjacent routers. If you configure transient mode for hello packets, these hello packets do not include the excess padding used before IS-IS establishes adjacencies. If the MTU value on adjacent routers changes, IS-IS can detect this change and send padded hello packets for a period of time. IS-IS uses this feature to detect mismatched MTU values on adjacent routers. For more information, see the “Configuring the Transient Mode for Hello Padding” section on page 9-21.</p> <p>IS-IS Areas</p> <p>You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. These Level 1/Level 2 routers act as area border routers that route information from the local area to the Level 2 backbone area (see Figure 9-1).</p> <p>Within a Level 1 area, routers know how to reach all other routers in that area. The Level 2 routers know how to reach other area border routers and other Level 2 routers. Level 1/Level 2 routers straddle the boundary between two areas, routing traffic to and from the Level 2 backbone area. Level 1/Level 2 routers use the attached (ATT) bit signal Level 1 routers to set a default route to this Level 1/Level 2 router to connect to the Level 2 area.</p> <p>In some instances, such as when you have two or more Level 1/Level 2 routers in an area, you may want to control which Level 1/Level 2 router that the Level 1 routers use as the default route to the Level 2 area. You can configure which Level 1/Level 2 router sets the attached bit. For more information, see the “Verifying the IS-IS Configuration” section on page 9-33.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-2.</p>	<p>IS-IS Description</p> <p>IS-IS sends a hello packet out every configured interface to discover IS-IS neighbor routers. The hello packet contains information, which the receiving interface uses to determine compatibility with the originating interface. Compatible interfaces form adjacencies, which update routing information in the link-state database through link-state update messages (LSPs). If the router does not receive an LSP refresh before the end of the LSP lifetime, the device deletes the LSP from the database.</p> <p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. IS-IS Areas – You can design IS-IS networks as a single area that includes all routers in the network or as multiple areas that connect into a backbone or Level 2 area. Routers in a nonbackbone area are Level 1 routers that establish adjacencies within a local area (intra-area routing). Level 2 area routers establish adjacencies to other Level 2 routers and perform routing between Level 1 areas (inter-area routing). A router can have both Level 1 and Level 2 areas configured. IS-IS Instances – Arista supports only one instance of the IS-IS protocol that run on the same node. LSP – Link state packet (LSP) can switch link state information. LSPs fall into two types: Level 1 LSPs and Level 2 LSPs. Level 2 devices transmit Level 2 LSPs; Level-1 devices transmit Level 1 LSPs; Level 1-2 devices transmit both Level 2 LSPs and Level 1 LSPs. Hello packets – Hello packets, can establish and maintain neighbor relationships. Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>NET and System ID</p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p>Designated Intermediate System</p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> Note No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-3.</p>	<p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>NET and System ID</p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p>Designated Intermediate System</p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> Note No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-3.</p>	<p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> • NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. • Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>NET and System ID</p> <p>Each IS-IS instance has an associated network entity title (NET). The NET is comprised of the IS-IS system ID, which uniquely identifies this IS-IS instance in the area and the area ID. For example, if the NET is 47.0004.004d.0001.0001.0c11.1111.00, the system ID is 0000.0c11.1111.00 and the area is ID 47.0004.004d.0001.</p> <p>Designated Intermediate System</p> <p>IS-IS uses a designated intermediate system (DIS) in broadcast networks to prevent each router from forming unnecessary links with every other router on the broadcast network. IS-IS routers send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area.</p> <p> Note No DIS is required on a point-to-point network.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-3.</p>	<p>Terms of IS-IS Routing Protocol</p> <p>The following terms are used when configuring IS-IS.</p> <ul style="list-style-type: none"> NET and System ID – Each IS-IS instance has an associated network entity title (NET). The NET consists of the IS-IS system ID, which uniquely identifies the IS-IS instance in the area and the area ID. Designated Intermediate System – IS-IS uses a Designated Intermediate System (DIS) in broadcast networks to prevent each device from forming unnecessary links with every other device on the broadcast network. IS-IS devices send LSPs to the DIS, which manages all the link-state information for the broadcast network. You can configure the IS-IS priority that IS-IS uses to select the DIS in an area. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>Overload Bit</p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> The router is in a critical condition. Graceful introduction and removal of the router to/from the network. Other (administrative or traffic engineering) reasons such as waiting for BGP convergence. <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-4.</p>	<ul style="list-style-type: none"> Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>
<p>Cisco NX-OS 5.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Overload Bit</p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> The router is in a critical condition. Graceful introduction and removal of the router to/from the network. Other (administrative or traffic engineering) reasons such as waiting for BGP convergence. <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 5.x (2010), at 9-4.</p>	<ul style="list-style-type: none"> Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 4.0</p> <p>Effective date of registration: 11/13/2014</p>	<p>Overload Bit</p> <p>IS-IS uses the overload bit to tell other routers not to use the local router to forward traffic but to continue routing traffic destined for that local router.</p> <p>You may want to use the overload bit in these situations:</p> <ul style="list-style-type: none"> • The router is in a critical condition. • Graceful introduction and removal of the router to/from the network. • Other (administrative or traffic engineering) reasons such as waiting for BGP convergence. <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 4.0 (2008), at 8-4.</p>	<ul style="list-style-type: none"> • Overload Bit – IS-IS uses the overload bit to tell other devices not to use the local router to forward traffic but to continue routing traffic destined for that local router. Possible conditions for setting the overload bit the device is in a critical condition. <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1674.</p> <p><i>See also</i> Arista User Manual v. 4.12.3 (7/17/13), at 1436.</p>

Copyright Registration Information	Cisco	Arista				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div><div>isis hello-multiplier num [level-1 level-2]</div><div>Example: switch(config-if)# isis hello-multiplier 20</div></div><div>Specifies the number of IS-IS hello packets that a neighbor must miss before the router tears down an adjacency. The range is from 3 to 1000. The default is 3.</div></div> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 9-33.</p>	<p>isis hello-multiplier</p> <p>The isis hello-multiplier command specifies the number of IS-IS hello packets a neighbor must miss before the device should declare the adjacency as down.</p> <p>Each hello packet contains a hold time. The hold time informs the receiving devices how long to wait without seeing another hello from the sending device before considering the sending device down. The isis hello-multiplier command is used to calculate the hold time announced in hello packets by multiplying this number with the configured isis hello-interval.</p> <p>The no isis hello-multiplier and default isis hello-multiplier commands restore the default hello interval of 3 on the configuration mode interface by removing the isis hello-multiplier command from running-config.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration</td></tr></table> <p>Command Syntax</p> <pre>isis hello-multiplier factor no isis hello-multiplier default isis hello-multiplier</pre> <p>Parameters</p> <ul style="list-style-type: none">factor hello multiplier. Values range from 3 to 100; default is 3 <p>Examples</p> <ul style="list-style-type: none">These commands configure a hello multiplier of 4 for VLAN 200. <pre>switch(config)#interface vlan 200 switch(config-if-Vl200)#isis hello-multiplier 4 switch(config-if-Vl200)#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1685.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1447.</p>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration
	Platform	all				
Command Mode	Interface-Ethernet Configuration Interface-Loopback Configuration Interface-Port-channel Configuration Interface-VLAN Configuration					

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="304 277 1142 375"> <p>Step 9 <code>route-reflector-client</code></p> <p>Example: <code>switch(config-router-neighbor-af) # route-reflector-client</code></p> </div> <p>Configures the device as a BGP route reflector and configures the neighbor as its client. This command triggers an automatic notification and session reset for the BGP neighbor sessions.</p> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 11-33.</p>	<p>A route reflector is configured to re-advertise routes learned through IBGP to a group of BGP neighbors within the AS (its clients), eliminating the need for a fully meshed topology. The <code>neighbor route-reflector-client</code> command configures the switch to act as a route reflector and configures the specified neighbor as one of its clients. The <code>bgp client-to-client reflection</code> command enables client-to-client reflection.</p> <p>When using route reflectors, an AS is divided into clusters. A cluster consists of one or more route reflectors and a group of clients to which they re-advertise route information. Multiple route reflectors can be configured in the same cluster to increase redundancy and avoid a single point of failure. Each route reflector has a cluster ID. If the cluster has a single route reflector, the cluster ID is its router ID. If a cluster has multiple route reflectors, a 4-byte cluster ID is assigned to all route reflectors in the cluster. All of them must be configured with the same cluster ID so that they can recognize updates from other route reflectors in the same cluster. The <code>bgp cluster-id</code> command configures the cluster ID in a cluster with multiple route reflectors.</p> <p>Example</p> <ul style="list-style-type: none"> These commands configure the switch as a route reflector and the neighbor at 101.72.14.5 as one of its clients, and set the cluster ID to 172.22.30.101. <div data-bbox="1247 688 1913 748"> <pre>switch(config-router-bgp) #neighbor 101.72.14.5 route-reflector-client switch(config-router-bgp) #bgp cluster-id 172.22.30.101 switch(config-router-bgp) #</pre> </div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1549.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1331; Arista User Manual, v. 4.11.1 (1/11/13), at 1081; Arista User Manual v. 4.10.3 (10/22/12), at 893; Arista User Manual v. 4.9.3.2 (5/3/12), at 665.</p>
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<div data-bbox="304 992 1142 1133"> <p>Static routes have a default administrative distance of 1. A router prefers a static route to a dynamic route because the router considers a route with a low number to be the shortest. If you want a dynamic route to override a static route, you can specify an administrative distance for the static route. For example, if you have two dynamic routes with an administrative distance of 120, you would specify an administrative distance that is greater than 120 for the static route if you want the dynamic route to override the static route.</p> </div> <p>Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide, Release 6.x (2013), at 13-2.</p>	<div data-bbox="1184 992 2028 1065"> <p>Static routes have a default administrative distance of 1. Static routes with a higher administrative distance may be overridden by dynamic routing. For example, a static route with a distance of 200 is overridden by default OSPF intra-area routes (distance of 110). Route maps use tags to filter routes.</p> </div> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1720.</p> <p>See also Arista User Manual v. 4.12.3 (7/17/13), at 1153; Arista User Manual, v. 4.11.1 (1/11/13), at 914; Arista User Manual v. 4.10.3 (10/22/12), at 683.</p>

Copyright Registration Information	Cisco	Arista																
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>clear ip igmp interface statistics</p> <p>To clear the IGMP statistics for an interface, use the <code>clear ip igmp interface statistics</code> command.</p> <p><code>clear ip igmp interface statistics</code> [<i>if-type if-number</i>]</p> <table border="1"> <tr> <td data-bbox="310 431 436 448">Syntax Description</td><td data-bbox="457 431 520 448"><i>if-type</i></td><td data-bbox="575 431 1136 467">(Optional) Interface type. For more information, use the question mark (?) online help function.</td></tr> <tr> <td></td><td data-bbox="457 475 531 492"><i>if-number</i></td><td data-bbox="575 475 1136 529">(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td></tr> </table> <p>Defaults None</p> <p>Command Modes Any command mode</p> <p>Supported User Roles network-admin network-operator vdc-admin vdc-operator</p> <table border="1"> <tr> <td data-bbox="310 837 426 854" rowspan="2">Command History</td><td data-bbox="457 837 520 854">Release</td><td data-bbox="627 837 716 854">Modification</td></tr> <tr> <td data-bbox="457 862 510 878">4.0(3)</td><td data-bbox="627 862 842 878">This command was introduced.</td></tr> </table> <p>Usage Guidelines This command does not require a license.</p> <p>Examples This example shows how to clear IGMP statistics for an interface:</p> <pre>switch# clear ip igmp interface statistics ethernet 2/1 switch#</pre> <table border="1"> <tr> <td data-bbox="310 1105 436 1122" rowspan="2">Related Commands</td><td data-bbox="457 1105 531 1122">Command</td><td data-bbox="627 1105 709 1122">Description</td></tr> <tr> <td data-bbox="457 1130 625 1146">show ip igmp interface</td><td data-bbox="627 1130 930 1146">Displays information about IGMP interfaces.</td></tr> </table> <p>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 6.</p>	Syntax Description	<i>if-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.		<i>if-number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.	Command History	Release	Modification	4.0(3)	This command was introduced.	Related Commands	Command	Description	show ip igmp interface	Displays information about IGMP interfaces.	<p>clear ip igmp statistics</p> <p>The <code>clear ip igmp statistics</code> command resets IGMP transmission statistic counters for the specified interface.</p> <p>Platform all</p> <p>Command Mode Privileged EXEC</p> <p>Command Syntax</p> <p><code>clear ip igmp statistics</code> [<i>INTF_ID</i>]</p> <p>Parameters</p> <ul style="list-style-type: none"> <i>INTF_ID</i> interface name. Options include: <ul style="list-style-type: none"> <no parameter> all interfaces. interface ethernet <i>e_num</i> Ethernet interface specified by <i>e_num</i>. interface loopback <i>l_num</i> Loopback interface specified by <i>l_num</i>. interface management <i>m_num</i> Management interface specified by <i>m_num</i>. interface port-channel <i>p_num</i> Port-channel interface specified by <i>p_num</i>. interface vlan <i>v_num</i> VLAN interface specified by <i>v_num</i>. interface xlan <i>vx_num</i> VXLAN interface specified by <i>vx_num</i>. <p>Examples</p> <ul style="list-style-type: none"> This command resets IGMP transmission statistic counters on Ethernet 1 interface. <pre>switch#clear ip igmp statistics interface ethernet 1 switch#</pre> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1794.</p>
Syntax Description	<i>if-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.																
	<i>if-number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.																
Command History	Release	Modification																
	4.0(3)	This command was introduced.																
Related Commands	Command	Description																
	show ip igmp interface	Displays information about IGMP interfaces.																

Copyright Registration Information	Cisco	Arista																								
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div>ip igmp snooping last-member-query-interval</div><div>To configure a query interval in which the software removes a group, use the <code>ip igmp snooping last-member-query-interval</code> command. To reset the query interval to the default, use the no form of this command.</div><div><div><code>ip igmp snooping last-member-query-interval [interval]</code></div><div><code>no ip igmp snooping last-member-query-interval [interval]</code></div></div><table><tr><td>Syntax Description</td><td><code>interval</code> Query interval in seconds. The range is from 1 to 25. The default is 1.</td></tr><tr><td>Defaults</td><td>The query interval is 1.</td></tr><tr><td>Command Modes</td><td>VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.</td></tr><tr><td>SupportedUserRoles</td><td>network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.</td></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></td></tr><tr><td>Usage Guidelines</td><td>This command does not require a license. See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.</td></tr><tr><td>Examples</td><td><div>This example shows how to configure a query interval in which the software removes a group: <code>switch(config)# vlan configuration 10</code> <code>switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3</code> <code>switch(config-vlan-config)#</code></div><div>This example shows how to reset a query interval to the default: <code>switch(config)# vlan configuration 10</code> <code>switch(config-vlan-config)# no ip igmp snooping last-member-query-interval</code> <code>switch(config-vlan-config)#</code></div></td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 86.</div></div>	Syntax Description	<code>interval</code> Query interval in seconds. The range is from 1 to 25. The default is 1.	Defaults	The query interval is 1.	Command Modes	VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.	SupportedUserRoles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.</td></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.	4.0(1)	This command was introduced.	Usage Guidelines	This command does not require a license. See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.	Examples	<div>This example shows how to configure a query interval in which the software removes a group: <code>switch(config)# vlan configuration 10</code> <code>switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3</code> <code>switch(config-vlan-config)#</code></div> <div>This example shows how to reset a query interval to the default: <code>switch(config)# vlan configuration 10</code> <code>switch(config-vlan-config)# no ip igmp snooping last-member-query-interval</code> <code>switch(config-vlan-config)#</code></div>	<div><div>ip igmp last-member-query-interval</div><div>The <code>ip igmp last-member-query-interval</code> command configures the switch's transmission interval for sending group-specific or group-source-specific query messages from the configuration mode interface.</div><div>When a switch receives a message from a host that is leaving a group it sends query messages at intervals set by this command. The <code>ip igmp startup-query-count</code> specifies the number of messages that are sent before the switch stops forwarding packets to the host.</div><div>If the switch does not receive a response after this period, it stops forwarding traffic to the host on behalf of the group, source, or channel.</div><div>The no <code>ip igmp last-member-query-interval</code> and default <code>ip igmp last-member-query-interval</code> commands reset the query interval to the default value of one second by removing the <code>ip igmp last-member-query-interval</code> command from <i>running-config</i>.</div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Port-Channel Configuration Interface-VLAN Configuration</td></tr></table><div>Command Syntax</div><div><div><code>ip igmp last-member-query-interval period</code></div><div><code>no ip igmp last-member-query-interval</code></div><div><code>default ip igmp last-member-query-interval</code></div></div><div>Parameters</div><div><ul style="list-style-type: none"><code>period</code> transmission interval (deciseconds) between consecutive group-specific query messages. Value range: 10 (one second) to 317440 (8 hours, 49 minutes, 4 seconds). Default is 10 (one second).</div><div>Example</div><div><ul style="list-style-type: none">This command configures the last member query interval of 6 seconds for VLAN interface 4. <code>switch(config)#interface vlan 4</code> <code>switch(config-if-Vl4)#ip igmp last-member-query-interval 60</code> <code>switch(config-if-Vl4)#</code></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1799.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1519; Arista User Manual, v. 4.11.1 (1/11/13), at 1216; Arista User Manual v. 4.10.3 (10/22/12), at 1000; Arista User Manual v. 4.9.3.2 (5/3/12), at 785.</div></div>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration Interface-VLAN Configuration
	Syntax Description	<code>interval</code> Query interval in seconds. The range is from 1 to 25. The default is 1.																								
Defaults	The query interval is 1.																									
Command Modes	VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.																									
SupportedUserRoles	network-admin vdc-admin																									
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>NX-OS 5.1(1)</td><td>The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.</td></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.	4.0(1)	This command was introduced.																			
Release	Modification																									
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.																									
4.0(1)	This command was introduced.																									
Usage Guidelines	This command does not require a license. See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.																									
Examples	<div>This example shows how to configure a query interval in which the software removes a group: <code>switch(config)# vlan configuration 10</code> <code>switch(config-vlan-config)# ip igmp snooping last-member-query-interval 3</code> <code>switch(config-vlan-config)#</code></div> <div>This example shows how to reset a query interval to the default: <code>switch(config)# vlan configuration 10</code> <code>switch(config-vlan-config)# no ip igmp snooping last-member-query-interval</code> <code>switch(config-vlan-config)#</code></div>																									
Platform	all																									
Command Mode	Interface-Ethernet Configuration Interface-Port-Channel Configuration Interface-VLAN Configuration																									

Copyright Registration Information	Cisco	Arista																																																														
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div><div>ip igmp snooping startup-query-count</div><div>To configure the number of queries sent at startup, use the ip igmp snooping startup-query-count command. To return to the default settings, use the no form of this command.</div><div><div>ip igmp snooping startup-query-count value</div><div>no ip igmp snooping startup-query-count value</div></div><table><tr><td>Syntax Description</td><td>value</td><td>Count value. The range is from 1 to 10.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">VLAN configuration (config-vlan)</td></tr><tr><td>SupportedUserRoles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to configure the number of queries sent at startup: switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#</td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 104.</div></div>	Syntax Description	value	Count value. The range is from 1 to 10.	Defaults	None		Command Modes	VLAN configuration (config-vlan)		SupportedUserRoles	network-admin vdc-admin		Command History	Release	Modification		NX-OS 5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure the number of queries sent at startup: switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#		Related Commands	Command	Description		show ip igmp snooping	Displays IGMP snooping information.	<div><div>ip igmp snooping querier startup-query-count</div><div>The ip igmp snooping querier startup-query-count command configures the global startup query count value. The startup query count specifies the number of query messages that the querier sends on a VLAN during the startup query interval (ip igmp snooping querier startup-query-interval).</div><div>When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The startup-query-interval and startup-query-count parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.</div><div>VLANs use the global startup query count value when they are not assigned a value (ip igmp snooping vlan querier startup-query-count). VLAN commands take precedence over the global value. The default global value is specified by the robustness variable (ip igmp snooping robustness-variable).</div><div>The no ip igmp snooping querier startup-query-count and default ip igmp snooping querier startup-query-count commands restore the default startup-query-count value by removing the corresponding ip igmp snooping querier startup-query-count command from running-config.</div><div>Platformall Command ModeGlobal Configuration</div><div>Command Syntax<div><div>ip igmp snooping querier startup-query-count number</div><div>no ip igmp snooping querier startup-query-count</div><div>default ip igmp snooping querier startup-query-count</div></div><div>Parameters<ul style="list-style-type: none">numberglobal startup query count. Value ranges from 1 to 3.</div><div>Example<ul style="list-style-type: none">These commands configure the global startup query count value of 2, then displays the status of the snooping querier.</div><div><div>switch(config)#ip igmp snooping querier startup-query-count 2</div><div>switch(config)#show ip igmp snooping querier status</div><div>Global IGMP Querier status</div><div>-----</div><div>admin state: Disabled</div><div>source IP address: 0.0.0.0</div><div>query-interval (sec): 125.0</div><div>max-response-time (sec): 10.0</div><div>querier timeout (sec): 255.0</div><div>last-member-query-interval (sec): 1.0</div><div>last-member-query-count: 2 (robustness)</div><div>startup-query-interval (sec): 31.25 (query-interval/4)</div><div>startup-query-count: 2</div><div>-----</div><table><tr><th>Vlan</th><th>Admin State</th><th>IP</th><th>Query Interval</th><th>Response Time</th><th>Querier Timeout</th><th>Operational State</th><th>Ver</th></tr><tr><td>1</td><td>Disabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v2</td></tr><tr><td>100</td><td>Disabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v2</td></tr><tr><td>101</td><td>Disabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v2</td></tr></table><div>switch(config)#</div></div></div></div>	Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver	1	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2	100	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2	101	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2
	Syntax Description	value	Count value. The range is from 1 to 10.																																																													
	Defaults	None																																																														
	Command Modes	VLAN configuration (config-vlan)																																																														
	SupportedUserRoles	network-admin vdc-admin																																																														
	Command History	Release	Modification																																																													
		NX-OS 5.1(1)	This command was introduced.																																																													
	Usage Guidelines	This command does not require a license.																																																														
	Examples	This example shows how to configure the number of queries sent at startup: switch(config)# vlan configuration 10 switch(config-vlan-config)# ip igmp snooping startup-query-count 4 switch(config-vlan-config)#																																																														
	Related Commands	Command	Description																																																													
	show ip igmp snooping	Displays IGMP snooping information.																																																														
Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver																																																									
1	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2																																																									
100	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2																																																									
101	Disabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v2																																																									

Copyright Registration Information	Cisco	Arista																																																														
<div></div> <div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip igmp snooping startup-query-interval</div><div>To configure the query interval at startup, use the <code>ip igmp snooping startup-query-interval</code> command. To return to the default settings, use the <code>no</code> form of this command.</div><div><div>ip igmp snooping startup-query-interval sec</div><div>no ip igmp snooping startup-query-interval sec</div></div><table><tr><td>Syntax Description</td><td>sec</td><td>Interval in seconds. The range is from 1 to 18000.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">VLAN configuration (config-vlan)</td></tr><tr><td>SupportedUserRoles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>NX-OS 5.1(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to configure the query interval at startup: switch(config)# <code>vlan configuration 10</code> switch(config-vlan-config)# <code>ip igmp snooping startup-query-interval 4</code> switch(config-vlan-config)#</td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 105.</div></div>	Syntax Description	sec	Interval in seconds. The range is from 1 to 18000.	Defaults	None		Command Modes	VLAN configuration (config-vlan)		SupportedUserRoles	network-admin vdc-admin		Command History	Release	Modification		NX-OS 5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure the query interval at startup: switch(config)# <code>vlan configuration 10</code> switch(config-vlan-config)# <code>ip igmp snooping startup-query-interval 4</code> switch(config-vlan-config)#		Related Commands	Command	Description		show ip igmp snooping	Displays IGMP snooping information.	<div><div>ip igmp snooping querier startup-query-interval</div><div>The <code>ip igmp snooping querier startup-query-interval</code> command configures the global startup query interval value. The <i>startup query interval</i> specifies the period between query messages that the querier sends upon startup.</div><div>When snooping is enabled, the group state is more quickly established by sending query messages at a higher frequency. The <i>startup-query-interval</i> and <i>startup-query-count</i> parameters define the startup period by defining the number of queries to be sent and transmission frequency for these messages.</div><div>VLANs use the global <i>startup query interval</i> value when they are not assigned a value (<code>ip igmp snooping vlan querier startup-query-interval</code>). VLAN commands take precedence over the global value. The default global value equals the query interval divided by four: (<code>ip igmp snooping querier query-interval</code>).</div><div>The <code>no ip igmp snooping querier startup-query-interval</code> and default <code>ip igmp snooping querier startup-query-interval</code> commands restore the default method of specifying the startup query interval by removing the corresponding <code>ip igmp snooping querier startup-query-interval</code> command from <i>running-config</i>.</div><div><div>Platform</div><div>all</div><div>Command Mode</div><div>Global Configuration</div></div><div>Command Syntax</div><div><div>ip igmp snooping querier startup-query-interval period</div><div>no ip igmp snooping querier startup-query-interval</div><div>default ip igmp snooping querier startup-query-interval</div></div><div>Parameters</div><div><div>•</div><div>period</div><div>startup query interval (seconds). Value ranges from 1 to 3600 (1 hour).</div></div><div>Example</div><div><div>•</div><div>This command configures the startup query count of one minute for VLAN interface 4.</div></div><div><div>switch(config)#ip igmp snooping querier startup-query-interval 40</div><div>switch(config)#show ip igmp snooping querier status</div><div>Global IGMP Querier status</div><div>-----</div><div>admin state : Enabled</div><div>source IP address : 0.0.0.0</div><div>query-interval (sec) : 125.0</div><div>max-response-time (sec) : 10.0</div><div>querier timeout (sec) : 255.0</div><div>last-member-query-interval (sec) : 1.0</div><div>last-member-query-count : 2 (robustness)</div><div>startup-query-interval (sec) : 40.0</div><div>startup-query-count : 2</div><div></div><div><table><tr><th>Vlan</th><th>Admin State</th><th>IP</th><th>Query Interval</th><th>Response Time</th><th>Querier Timeout</th><th>Operational State</th><th>Ver</th></tr><tr><td>1</td><td>Enabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v3</td></tr><tr><td>100</td><td>Enabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v3</td></tr><tr><td>101</td><td>Enabled</td><td>0.0.0.0</td><td>125.0</td><td>10.0</td><td>255.0</td><td>Non-Querier</td><td>v3</td></tr></table></div><div>switch(config)#</div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1813.</div></div>	Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver	1	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3	100	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3	101	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3
	Syntax Description	sec	Interval in seconds. The range is from 1 to 18000.																																																													
Defaults	None																																																															
Command Modes	VLAN configuration (config-vlan)																																																															
SupportedUserRoles	network-admin vdc-admin																																																															
Command History	Release	Modification																																																														
	NX-OS 5.1(1)	This command was introduced.																																																														
Usage Guidelines	This command does not require a license.																																																															
Examples	This example shows how to configure the query interval at startup: switch(config)# <code>vlan configuration 10</code> switch(config-vlan-config)# <code>ip igmp snooping startup-query-interval 4</code> switch(config-vlan-config)#																																																															
Related Commands	Command	Description																																																														
	show ip igmp snooping	Displays IGMP snooping information.																																																														
Vlan	Admin State	IP	Query Interval	Response Time	Querier Timeout	Operational State	Ver																																																									
1	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3																																																									
100	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3																																																									
101	Enabled	0.0.0.0	125.0	10.0	255.0	Non-Querier	v3																																																									

Copyright Registration Information	Cisco	Arista																														
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div><div>ip igmp snooping version</div><div>To configure the IGMP version number for VLAN, use the ip igmp snooping version command. To return to the default settings, use the no form of this command.</div><div><div>ip igmp snooping version value</div><div>no ip igmp snooping version value</div></div></div><table><tr><td>Syntax Description</td><td>value</td><td>Version number value. The range is from 2 to 3.</td></tr><tr><td>Defaults</td><td colspan="2">None</td></tr><tr><td>Command Modes</td><td colspan="2">VLAN configuration (config-vlan)</td></tr><tr><td>SupportedUserRoles</td><td colspan="2">network-admin vdc-admin</td></tr><tr><td>Command History</td><td>Release</td><td>Modification</td></tr><tr><td></td><td>5.1(1)</td><td>This command was introduced.</td></tr><tr><td>Usage Guidelines</td><td colspan="2">This command does not require a license.</td></tr><tr><td>Examples</td><td colspan="2">This example shows how to configure IGMP version number for VLAN:<div>switch(config-vlan-config)# ip igmp snooping version 3 switch(config-vlan-config)#</div></td></tr><tr><td>Related Commands</td><td>Command</td><td>Description</td></tr><tr><td></td><td>show ip igmp snooping</td><td>Displays IGMP snooping information.</td></tr></table><div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 108.</div></div>	Syntax Description	value	Version number value. The range is from 2 to 3.	Defaults	None		Command Modes	VLAN configuration (config-vlan)		SupportedUserRoles	network-admin vdc-admin		Command History	Release	Modification		5.1(1)	This command was introduced.	Usage Guidelines	This command does not require a license.		Examples	This example shows how to configure IGMP version number for VLAN: <div>switch(config-vlan-config)# ip igmp snooping version 3 switch(config-vlan-config)#</div>		Related Commands	Command	Description		show ip igmp snooping	Displays IGMP snooping information.	<div><div><div>ip igmp snooping querier version</div><div>The ip igmp snooping querier version command configures the Internet Group Management Protocol (IGMP) snooping querier version on the configuration mode interfaces. Version 3 is the default IGMP version.</div><div>IGMP is enabled by the ip pim sparse-mode command. The ig igmp snooping querier version command does not affect the IGMP enabled status.</div><div>The no ip igmp snooping querier version and default ip igmp snooping querier version commands restore the configuration mode to IGMP version 3 by removing the ip igmp snooping querier version statement from running-config.</div><div><div>Platformall</div><div>Command ModeGlobal Configuration</div></div><div>Command Syntax<div><div>ip igmp snooping querier version version_number</div><div>no ip igmp snooping querier version</div><div>default ip igmp snooping querier version</div></div></div><div>Parameters<ul style="list-style-type: none">version_numberIGMP version number. Value ranges from 1 to 3. Default value is 3.</div><div>Example<ul style="list-style-type: none">This command configures IGMP snooping querier version 2.<div>switch(config)#ip igmp snooping querier version 2 switch(config)#</div>This command restores the IGMP snooping querier to version 2.<div>switch(config)# no ip igmp snooping querier version switch(config)#</div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1815.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1531.</div></div></div>
	Syntax Description	value	Version number value. The range is from 2 to 3.																													
Defaults	None																															
Command Modes	VLAN configuration (config-vlan)																															
SupportedUserRoles	network-admin vdc-admin																															
Command History	Release	Modification																														
	5.1(1)	This command was introduced.																														
Usage Guidelines	This command does not require a license.																															
Examples	This example shows how to configure IGMP version number for VLAN: <div>switch(config-vlan-config)# ip igmp snooping version 3 switch(config-vlan-config)#</div>																															
Related Commands	Command	Description																														
	show ip igmp snooping	Displays IGMP snooping information.																														

Copyright Registration Information	Cisco	Arista																																				
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>Examples</div> <div>This example shows how to display information about IGMP snooping queriers:</div> <div><pre>switch(config)# show ip igmp snooping querier</pre><table><tr><th>Vlan</th><th>IP Address</th><th>Version</th><th>Port</th></tr><tr><td>1</td><td>172.20.50.11</td><td>v3</td><td>fa2/1</td></tr><tr><td>2</td><td>172.20.40.20</td><td>v2</td><td>Router</td></tr></table><pre>switch(config)#</pre></div> <div>Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference (2013), at 50.</div>	Vlan	IP Address	Version	Port	1	172.20.50.11	v3	fa2/1	2	172.20.40.20	v2	Router	<div>Example</div> <div><ul style="list-style-type: none">This command displays the querier IP address, version, and port servicing each VLAN.</div> <div><pre>switch>show ip igmp snooping querier</pre><table><tr><th>Vlan</th><th>IP Address</th><th>Version</th><th>Port</th></tr><tr><td colspan="4">-----</td></tr><tr><td>1</td><td>172.17.0.37</td><td>v2</td><td>Pol</td></tr><tr><td>20</td><td>172.17.20.1</td><td>v2</td><td>Pol</td></tr><tr><td>26</td><td>172.17.26.1</td><td>v2</td><td>Cpu</td></tr><tr><td>2028</td><td>172.17.255.29</td><td>v2</td><td>Pol</td></tr></table><pre>switch></pre></div> <div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1860.</div> <div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1568; Arista User Manual, v. 4.11.1 (1/11/13), at 1263; Arista User Manual v. 4.10.3 (10/22/12), at 1074; Arista User Manual v. 4.9.3.2 (5/3/12), at 831; Arista User Manual v. 4.8.2 (11/18/11), at 637.</div>	Vlan	IP Address	Version	Port	-----				1	172.17.0.37	v2	Pol	20	172.17.20.1	v2	Pol	26	172.17.26.1	v2	Cpu	2028	172.17.255.29	v2	Pol
	Vlan	IP Address	Version	Port																																		
1	172.20.50.11	v3	fa2/1																																			
2	172.20.40.20	v2	Router																																			
Vlan	IP Address	Version	Port																																			

1	172.17.0.37	v2	Pol																																			
20	172.17.20.1	v2	Pol																																			
26	172.17.26.1	v2	Cpu																																			
2028	172.17.255.29	v2	Pol																																			

Copyright Registration Information	Cisco	Arista																									
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>aaa group server tacacs+</div><div>To create a TACACS+ server group and enter TACACS+ server group configuration mode, use the <code>aaa group server tacacs+</code> command. To delete a TACACS+ server group, use the <code>no</code> form of this command.</div><div>aaa group server tacacs+ group-name</div><div>no aaa group server tacacs+ group-name</div><div><table><tr><td>Syntax Description</td><td>group-name</td><td>TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.</td></tr></table></div><div><table><tr><td>Defaults</td><td>None</td></tr></table></div><div><table><tr><td>Command Modes</td><td>Global configuration</td></tr></table></div><div><table><tr><td>SupportedUserRoles</td><td>network-admin vdc-admin</td></tr></table></div><div><table><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></td></tr></table></div><div><table><tr><td>Usage Guidelines</td><td>You must use the <code>feature tacacs+</code> command before you configure TACACS+.</td></tr><tr><td></td><td>This command does not require a license.</td></tr></table></div><div><table><tr><td>Examples</td><td><div>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</div><div>switch# configure terminal</div><div>switch(config)# aaa group server tacacs+ TacServer</div><div>switch(config-radius)#</div><div>This example shows how to delete a TACACS+ server group:</div><div>switch# configure terminal</div><div>switch(config)# no aaa group server tacacs+ TacServer</div></td></tr></table></div></div>	Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.	Defaults	None	Command Modes	Global configuration	SupportedUserRoles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.	Usage Guidelines	You must use the <code>feature tacacs+</code> command before you configure TACACS+.		This command does not require a license.	Examples	<div>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</div> <div>switch# configure terminal</div> <div>switch(config)# aaa group server tacacs+ TacServer</div> <div>switch(config-radius)#</div> <div>This example shows how to delete a TACACS+ server group:</div> <div>switch# configure terminal</div> <div>switch(config)# no aaa group server tacacs+ TacServer</div>	<div><div>aaa group server tacacs+</div><div>The <code>aaa group server tacacs+</code> command enters <code>server-group-tacacs+</code> configuration mode for the specified group name. The command creates the specified group if it was not previously created. Commands are available to add servers to the group.</div><div>A server group is a collection of servers that are associated with a single label. Subsequent authorization and authentication commands access all servers in a group by invoking the group name. Server group members must be previously configured with a <code>tacacs-server host</code> command.</div><div>The <code>no aaa group server tacacs+</code> and default <code>aaa group server tacacs+</code> commands delete the specified server group from <i>running-config</i>.</div><div><table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Global Configuration</td></tr></table></div><div>Command Syntax<div>aaa group server tacacs+ group_name</div><div>no aaa group server tacacs+ group_name</div><div>default aaa group server tacacs+ group_name</div></div><div>Parameters<ul style="list-style-type: none"><code>group_name</code> name (text string) assigned to the group. Cannot be identical to a name already assigned to a RADIUS server group.</div><div>Commands Available in <code>server-group-tacacs+</code> Configuration Mode<ul style="list-style-type: none"><code>server (server-group-TACACS+ configuration mode)</code></div><div>Related Commands<ul style="list-style-type: none"><code>aaa group server radius</code></div><div>Example<ul style="list-style-type: none">This command creates the TACACS+ server group named TAC-GR and enters server group configuration mode for the new group.<div>switch(config)#aaa group server tacacs+ TAC-GR</div><div>switch(config-sg-tacacs+-TAC-GR)#</div></div></div>	Platform	all	Command Mode	Global Configuration
	Syntax Description	group-name	TACACS+ server group name. The name is alphanumeric and case-sensitive. The maximum length is 64 characters.																								
Defaults	None																										
Command Modes	Global configuration																										
SupportedUserRoles	network-admin vdc-admin																										
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.0(1)	This command was introduced.																						
Release	Modification																										
4.0(1)	This command was introduced.																										
Usage Guidelines	You must use the <code>feature tacacs+</code> command before you configure TACACS+.																										
	This command does not require a license.																										
Examples	<div>This example shows how to create a TACACS+ server group and enter TACACS+ server configuration mode:</div> <div>switch# configure terminal</div> <div>switch(config)# aaa group server tacacs+ TacServer</div> <div>switch(config-radius)#</div> <div>This example shows how to delete a TACACS+ server group:</div> <div>switch# configure terminal</div> <div>switch(config)# no aaa group server tacacs+ TacServer</div>																										
Platform	all																										
Command Mode	Global Configuration																										

Copyright Registration Information	Cisco	Arista																						
Cisco NX-OS 6.2 Effective date of registration: 11/13/2014	<div>dot1x pae authenticator</div> <p>To create the 802.1X authenticator port access entity (PAE) role for an interface, use the <code>dot1x pae authenticator</code> command. To remove the 802.1X authenticator PAE role, use the <code>no</code> form of this command.</p> <div>dot1x pae authenticator</div> <div>no dot1x pae authenticator</div> <table><tr><td>Syntax Description</td><td>This command has no arguments or keywords.</td></tr><tr><td>Defaults</td><td>802.1X automatically creates the authenticator PAE when you enable the feature on an interface.</td></tr><tr><td>Command Modes</td><td>Interface configuration</td></tr><tr><td>SupportedUserRoles</td><td>network-admin vdc-admin</td></tr><tr><td>Command History</td><td><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.2(1)</td><td>This command was introduced.</td></tr></table></td></tr><tr><td>Usage Guidelines</td><td><p>You must use the <code>feature dot1x</code> command before you configure 802.1X.</p><p>When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.</p><p>This command does not require a license.</p></td></tr><tr><td>Examples</td><td><p>This example shows how to create the 802.1X authenticator PAE role on an interface:</p><pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# dot1x pae authenticator</pre><p>This example shows how to remove the 802.1X authenticator PAE role from an interface:</p><pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# no dot1x pae authenticator</pre></td></tr></table>	Syntax Description	This command has no arguments or keywords.	Defaults	802.1X automatically creates the authenticator PAE when you enable the feature on an interface.	Command Modes	Interface configuration	SupportedUserRoles	network-admin vdc-admin	Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.2(1)	This command was introduced.	Usage Guidelines	<p>You must use the <code>feature dot1x</code> command before you configure 802.1X.</p> <p>When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.</p> <p>This command does not require a license.</p>	Examples	<p>This example shows how to create the 802.1X authenticator PAE role on an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# dot1x pae authenticator</pre> <p>This example shows how to remove the 802.1X authenticator PAE role from an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# no dot1x pae authenticator</pre>	<div>dot1x pae authenticator</div> <p>The <code>dot1x pae authenticator</code> command sets the Port Access Entity (PAE) type. The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.</p> <p>The <code>no dot1x pae authenticator</code> and default <code>dot1x pae authenticator</code> commands restore the switch default by deleting the corresponding <code>dot1x pae authenticator</code> command from <i>running-config</i>.</p> <table><tr><td>Platform</td><td>all</td></tr><tr><td>Command Mode</td><td>Interface-Ethernet Configuration Interface-Management Configuration</td></tr></table> <p>Command Syntax</p> <div>dot1x pae authenticator</div> <div>no dot1x pae authenticator</div> <div>default dot1x pae authenticator</div> <p>Example</p> <ul style="list-style-type: none">This command configures the port as an IEEE 802.1x port access entity (PAE) authenticator, which enables IEEE 802.1x on the port but does not allow clients connected to the port to be authorized, use the <code>dot1x pae authenticator</code> interface configuration command. <pre>switch(config-if-Et1)#interface ethernet 2 switch(config-if-Et1)#dot1x pae authenticator switch(config-if-Et1)#</pre> <ul style="list-style-type: none">This example shows how to disable IEEE 802.1x authentication on the port. <pre>switch(config-if-Et1)#interface ethernet 2 switch(config-if-Et1)#no dot1x pae authenticator switch(config-if-Et1)#</pre>	Platform	all	Command Mode	Interface-Ethernet Configuration Interface-Management Configuration
	Syntax Description	This command has no arguments or keywords.																						
Defaults	802.1X automatically creates the authenticator PAE when you enable the feature on an interface.																							
Command Modes	Interface configuration																							
SupportedUserRoles	network-admin vdc-admin																							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.2(1)</td><td>This command was introduced.</td></tr></table>	Release	Modification	4.2(1)	This command was introduced.																			
Release	Modification																							
4.2(1)	This command was introduced.																							
Usage Guidelines	<p>You must use the <code>feature dot1x</code> command before you configure 802.1X.</p> <p>When you enable 802.1X on an interface, the Cisco NX-OS software creates an authenticator port access entity (PAE) instance. An authenticator PAE is a protocol entity that supports authentication on the interface. When you disable 802.1X on the interface, the Cisco NX-OS software does not automatically clear the authenticator PAE instances. You can explicitly remove the authenticator PAE from the interface and then reapply it, as needed.</p> <p>This command does not require a license.</p>																							
Examples	<p>This example shows how to create the 802.1X authenticator PAE role on an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# dot1x pae authenticator</pre> <p>This example shows how to remove the 802.1X authenticator PAE role from an interface:</p> <pre>switch# configure terminal switch(config)# interface ethernet 2/4 switch(config-if)# no dot1x pae authenticator</pre>																							
Platform	all																							
Command Mode	Interface-Ethernet Configuration Interface-Management Configuration																							

Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 566.

Copyright Registration Information	Cisco	Arista
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>dot1x timeout quiet-period</div><div><p>To configure the 802.1X quiet-period timeout globally or for an interface, use the <code>dot1x timeout quiet-period</code> command. To revert to the default, use the <code>no</code> form of this command.</p><div><div>dot1x timeout quiet-period seconds</div><div>no dot1x timeout quiet-period</div></div></div><div><div><div>Syntax Description</div><div>seconds</div><div>Number of seconds for the 802.1X quiet-period timeout. The range is from 1 to 65535.</div></div><div><div>Defaults</div><div>Global configuration: 60 seconds Interface configuration: The value of the global configuration</div></div><div><div>Command Modes</div><div>Global configuration Interface configuration</div></div><div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div><div><div><div>Command History</div><div><div>Release</div><div>Modification</div></div><div><div>4.0(1)</div><div>This command was introduced.</div></div></div></div><div><div><div>Usage Guidelines</div><div><p>The 802.1X quiet-period timeout is the number of seconds that the device remains in the quiet state following a failed authentication exchange with a supplicant.</p><p>You must use the <code>feature dot1x</code> command before you configure 802.1X.</p><div><div>Note</div><div><p>You should change the default value only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain supplicants and authentication servers.</p><p>This command does not require a license.</p></div></div></div></div><div><div><div>Examples</div><div><p>This example shows how to configure the global 802.1X quiet-period timeout:</p><pre>switch# configure terminal switch(config)# dot1x timeout quiet-period 45</pre></div></div></div></div></div></div>	<div><div>dot1x timeout quiet-period</div><div><p>The <code>dot1x timeout quiet-period</code> command sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.</p><p>When the switch cannot authenticate the client, the switch remains idle for a set period of time and then tries again. You can provide a faster response time to the user by entering a number smaller than the default.</p><p>The <code>no dot1x timeout quiet-period</code> and default <code>dot1x timeout quiet-period</code> commands restore the default advertisement interval of 60 seconds by removing the corresponding <code>dot1x timeout quiet-period</code> command from <i>running-config</i>.</p><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Interface-Ethernet Configuration Interface-Management Configuration</div></div><div><div>Command Syntax</div><div><pre>dot1x timeout quiet-period quiet_time no dot1x timeout quiet-period default dot1x timeout quiet-period</pre></div></div><div><div>Parameters</div><div><ul style="list-style-type: none"><code>quiet_time</code> advertisement interval (seconds). Values range from 1 to 65535. Default value is 60.</div></div><div><div>Example</div><div><ul style="list-style-type: none">This command sets the number of seconds that an authenticator port waits after a failed authentication with a client before accepting authentication requests again.<pre>switch(config)#interface Ethernet 1 switch(config-if-Et1)#dot1x timeout quiet-period 600 switch(config-if-Et1)#</pre></div></div></div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 569.</div></div>

Copyright Registration Information	Cisco	Arista
<p>Cisco NX-OS 6.2</p> <p>Effective date of registration: 11/13/2014</p>	<p>To use this command, you must enable the DHCP snooping feature (see the <code>feature dhcp</code> command). You can configure up to four DHCP server IP addresses on Layer 3 Ethernet interfaces and subinterfaces, VLAN interfaces, and Layer 3 port channels. In Cisco NX-OS Release 4.0.2 and earlier releases, you can configure only one DHCP server IP address on an interface.</p> <p>When an inbound DHCP BOOTREQUEST packet arrives on the interface, <u>the relay agent forwards the packet to all DHCP server IP addresses specified on that interface. The relay agent forwards replies from all DHCP servers to the host that sent the request.</u></p> <p>This command does not require a license.</p> <p>Cisco Nexus 7000 Series NX-OS Security Command Reference (2013), at SEC-309.</p>	<p>The <code>ip dhcp snooping information option</code> command enables the insertion of option-82 DHCP snooping information in DHCP packets on VLANs where DHCP snooping is enabled. DHCP snooping is a layer 2 switch process that allows relay agents to provide remote-ID and circuit-ID information to DHCP reply and request packets. DHCP servers use this information to determine the originating port of DHCP requests and associate a corresponding IP address to that port.</p> <p>DHCP snooping uses information option (Option-82) to include the switch MAC address (router-ID) along with the physical interface name and <u>VLAN number (circuit-ID)</u> in DHCP packets. After adding the information to the packet, <u>the DHCP relay agent forwards the packet to the DHCP server</u> through DHCP protocol processes.</p> <p>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1270.</p>

Copyright Registration Information	Cisco	Arista														
<div>Cisco NX-OS 6.2</div> <div>Effective date of registration: 11/13/2014</div>	<div><div>ip dhcp relay information option</div><div>To enable the device to insert and remove option-82 information on DHCP packets forwarded by the relay agent, use the <code>ip dhcp relay information option</code> command. To disable the insertion and removal of option-82 information, use the <code>no</code> form of this command.</div><div><div>ip dhcp relay information option</div><div>no ip dhcp relay information option</div></div><div><div>Syntax Description</div><div>This command has no arguments or keywords.</div></div><div><div>Defaults</div><div>By default, the device does not insert and remove option-82 information on DHCP packets forwarded by the relay agent.</div></div><div><div>Command Modes</div><div>Global configuration</div></div><div><div>SupportedUserRoles</div><div>network-admin vdc-admin</div></div><div><div>Command History</div><table><tr><th>Release</th><th>Modification</th></tr><tr><td>4.0(1)</td><td>This command was introduced.</td></tr></table></div><div><div>Usage Guidelines</div><div>To use this command, you must enable the DHCP snooping feature (see the <code>feature dhcp</code> command). This command does not require a license.</div></div><div><div>Examples</div><div><div>This example shows how to enable the DHCP relay agent to insert and remove option-82 information to and from packets it forwards:</div><div>switch# configure terminal Switch(config)# ip dhcp relay information option switch(config)#</div></div></div><div><div>Related Commands</div><table><tr><th>Command</th><th>Description</th></tr><tr><td>ip dhcp relay</td><td>Enables or disables the DHCP relay agent.</td></tr><tr><td>ip dhcp relay address</td><td>Configures the IP address of a DHCP server on an interface.</td></tr><tr><td>ip dhcp relay sub-option type cisco</td><td>Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.</td></tr><tr><td>ip dhcp snooping</td><td>Globally enables DHCP snooping on the device.</td></tr></table></div></div>	Release	Modification	4.0(1)	This command was introduced.	Command	Description	ip dhcp relay	Enables or disables the DHCP relay agent.	ip dhcp relay address	Configures the IP address of a DHCP server on an interface.	ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.	ip dhcp snooping	Globally enables DHCP snooping on the device.	<div><div>ip dhcp relay information option (Global)</div><div>The <code>ip dhcp relay information option</code> command configures the switch to attach tags to DHCP requests before forwarding them to the DHCP servers designated by <code>ip helper-address</code> commands. The <code>ip dhcp relay information option circuit-id</code> command specifies the tag contents for packets forwarded by the interface that it configures.</div><div>The no <code>ip dhcp relay information option</code> and default <code>ip dhcp relay information option</code> commands restore the switch's default setting of not attaching tags to DHCP requests by removing the <code>ip dhcp relay information option</code> command from <i>running-config</i>.</div><div><div>Platform</div><div>all</div></div><div><div>Command Mode</div><div>Global Configuration</div></div><div><div>Command Syntax</div><div><div>ip dhcp relay information option</div><div>no ip dhcp relay information option</div><div>default ip dhcp relay information option</div></div></div><div><div>Related Commands</div><div>These commands implement DHCP relay agent.</div><div><ul style="list-style-type: none">ip helper-addressip dhcp relay always-onip dhcp relay information option circuit-id</div></div><div><div>Example</div><div><ul style="list-style-type: none">This command enables the attachment of tags to DHCP requests that are forwarded to DHCP server addresses.<div>switch(config)#ip dhcp relay information option switch(config)#</div></div></div><div><div>Arista User Manual v. 4.14.3F – Rev. 2 (10/2/2014), at 1264.</div><div>See also Arista User Manual v. 4.12.3 (7/17/13), at 1068; Arista User Manual, v. 4.11.1 (1/11/13), at 852; Arista User Manual v. 4.10.3 (10/22/12), at 701.</div></div></div>
	Release	Modification														
4.0(1)	This command was introduced.															
Command	Description															
ip dhcp relay	Enables or disables the DHCP relay agent.															
ip dhcp relay address	Configures the IP address of a DHCP server on an interface.															
ip dhcp relay sub-option type cisco	Enables DHCP to use Cisco proprietary numbers 150, 152, and 151 when filling the link selection, server ID override, and VRF name/VPN ID relay agent option-82 suboptions.															
ip dhcp snooping	Globally enables DHCP snooping on the device.															